Galois theory

Jeroen Sijsling

May 17, 2024

Contents

Introduction

> C'est que, malheureusement, on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté.
>
> — Évariste Galois (1811–1832), in his preface to *Deux mémoires d'analyse pure*.

These are the lecture notes for Galois theory at Ulm University. They should be accessible after either of the courses Algebra and Elemente der Algebra. It consists mainly of a more detailed investigation of the structure of field extensions, and provides an especially pleasing way to understand these in terms of group theory.

In some university systems, and in Germany in particular, Galois theory is a highly fetishized topic, which is not only held up as the pinnacle of austere beauty towards which every other algebraic theory should strive, but also as both a sina qua non and the nec plus ultra of undergraduate algebra courses. This is sterile dogmatics; as omnia munda mundis, so too does any mathematical result contain the deepest profundities to those who know where to look. Galois theory is not the unique source of such revelations, though it most definitely has never ceased to inspire and astonish later mathematicians, as Michael Harris mentions in his statement above.

These notes instead take a more concrete view of Galois theory, namely as a highly useful tool to deepen one's understanding of field extensions by provided a translations of their properties into the language of group theory. We therefore motivate all the field-theoretic notions that go into the notion of a Galois extension, and show where these notions play a role in practice, instead of restricting ourselves to theory. (In a sense, you will see how you would, given enough time, have invented the whole yourself.) In addition, these notes do not close their eyes to situations where Galois theory will indicate a solution that may be highly satisfying in the abstract, but that is more difficult in concrete situations than it would at first let on. In other words, we treat Galois theory both with the same esteem and with the same critical spirit as any other part of mathematics.

Since our approach aims to show the role of Galois theory in modern mathematics, the full details around some themes have fallen by the wayside. In particular, this is true for the problem of describing field extensions by means of radicals, which led Galois to develop his eponymous theory. However, this theme remains as one of the projects at the end of this course. Moreover, we will describe this saga and other parts of the historical background of Galois theory in remarks scattered throughout these notes. Though Galois theory does not outrank its peers, the story behind it, as well as the theories that it in turn inspired, are intertwined with some of the most fascinating stories in mathematics.

A very brief summary of these notes is as follows. In Chapters I and II, we consider the notions of normality and separability for field extensions, and show how these occur naturally in practice. Combining these leads to Galois extensions, which we study in Chapter III. It turns out that (finite) Galois extensions are exactly those field extensions that are highly symmetric, in the sense that their automorphism group is as large as it can be. So large, in fact, are the automorphism groups of Galois extensions, that they can be used to completely describe the subfields of such extensions and their properties, as we shall see in Chapter IV. This delightful result is known as the main theorem of Galois theory.

In Chapter V, we consider the results around the main theorem in a somewhat more constructive fashion, and we discuss how these can be transferred from the realm of theory to that of concrete computations. After this, we discuss some of the many applications of Galois theory in Chapter VI. Finally, the concluding Chapter VII contains a number of advanced projects that explore Galois theory further, and that can be explored in the form of a common project.

Far more motivation can be found in the introduction to the chapters themselves. Be sure also to read the upcoming sections on the structure of the notes and the course itself, since this is essential for successful and productive participation.

The structure of the course

You have probably already seen that these notes are relatively long and elaborate. However, the aim of the course is not to memorize all their pages, or even to read them in full. These notes are not the definitive, maximally abbreviated summary of its material, but part of the support material for the corresponding course. This section explains how the different components of this course relate to each other, and what role these lecture notes play in it.

The material of the course is basically divided into weekly sections, and each week is organized as follows:

(i) Before the start of the week, you will be told what the material will be and what the most important related results in the notes are. At this point, you can already orient yourself to what will happen during the week.

(ii) At the beginning of the week, a short, conceptually oriented video is uploaded first. It briefly explains and motivates what is to come. Details

are not covered in this video, as this is part of the next steps. Instead, this video is your **first, motivating** encounter with the material; it explains its underlying ideas as well as their underlying why.

(iii) It is then up to you to encounter the material yourself for the first time by reading through the notes before the weekly lectures. This is the beginning of the **second, in-depth** encounter with the material, i.e. the encounter with some of its more subtle details. For this purpose, additional videos are provided, in which this material is discussed more eloborately. These videos are a tool that you can use as you wish; you can use them before, during or after reading.

(iv) In the lectures themselves, the material is repeated and summarized, and then further explained using concrete examples. Note that the lecture will not necessarily cover all the details of more complicated proofs; this only happens if they help for understanding the material. Regardless, the details are always available in the weekly videos. Instead, the aim of the lecture is to activate and illustrate the knowledge that you will have absorbed so far.

(v) An important component of the lecture is interaction. During this you can ask questions of any kind, and also ask for more examples around the week's material. Conversely, you (i.e. the audience as a whole) will also be asked questions from time to time, either to activate your knowledge or to see how the material was absorbed.

(vi) After the last lecture of the week, there is an online quiz that is part of the Vorleistung. This contains some conceptual questions about the material. Some questions are simple, some are more complicated, and some, dealing with fine-grained subtleties, are even a little mean. Their purpose is to conclude the further and deeper encounter with the material that takes place around the lecture with a final reflection. Along with the renewed confrontation the week's topics at later occasions, these quiz are part of the **third, integrative** encounter with the material; this final active encounter shows the role of its topics and results in the larger mathematical whole beyond the often abstract context in which you first encounter it. After all, that is where you will use it later.

There are many components to this weekly program, and it is clear that time pressure is always present during your studies. This sometimes makes it impossible to do everything you would like to do. The remainder of this section discusses what exactly is expected of you and what is not, and how you can participate in the course in a productive and insightful way.

The first encounter with the weekly material, which serves as an orientation, as discussed in Parts (i)-(ii) above, takes very little time; it is enough to briefly browse through the material and watch the short, motivational video. It is simply not worth skipping this part. You can also take part in the weekly lecture with this bare minimum.

The second encounter with the material includes the reading, the videos, and the weekly lectures to deepen your understanding. It is not absolutely necessary

to use all these components. Part (iii) in particular is time-consuming, and as an alternative you can also just read through the specified sections of the notes before the lecture, and only watch the parts of the videos that relate to the parts of the notes where your understanding needs some supplementation.

Yet the more you uses these resources, the more they will pay off. Moreover, the aforementioned bare minimum, where you do not engage with either the notes or the videos before the lectures, is a real minimum; it is therefore an option in one or two particularly busy weeks, but it is **not** recommended in the long run, especially as the lectures assume that you are already aware of the themes discussed in them.

As for the lecture itself, i.e. Parts (iv)-(v) above, the more actively you participate, the better. Your feedback will allow me to take your personal needs into account at all times. Also note that you do not necessarily have to take notes from the blackboard in the lectures, as all relevant results and examples are already included in the notes. However, many find taking notes helpful and mentally stimulating, and of course you will never be prohibited from doing so. The converse holds for participation to questions and discussions during the lecture; it is very useful, and I appreciate all answers and feedback, but you do not necessarily have to participate.

The immersion in the lecture does not complete the learning process by itself. The third encounter with the material, as described in part (vi) above, serves to integrate the abstract knowledge into your mathematical education as a whole. This is the most important and probably the most difficult aspect of any course. No lecture or notes exist, no matter how well structured, that can in themselves convey what can only be gained through active participation and practice. The exercises are designed to help with this, and indicate cross-connections that exist between the different parts of the theory that are incredibly useful, but they require time and mental engagement to understand and absorb.

However, it is only in this last, integrative part that the actual mathematical education takes place and the material is transformed from a mechanical abstract concept into a source of active enquiring knowledge. Abstraction in itself is the great power of mathematics… but it is understanding that is its purpose. This is also why the notes are designed in the way that they are, and why they are not their own lean and minimal summary. Here and there a story is told, a detailed example elaborated, a new perspective presented, a success savored, an exaltation indulged in. Some remark in these notes are strictly speaking unnecessary, but then again there are many aspects of life that are strictly speaking unnecessary, and without which it would be rather cold, dark, and pointless.

So go through the notes slowly, as they are presented and elaborated upon in the course. The first time you read it, only part of it will be discussed, and you do not have to understand or even read all the examples at once. Much of it will simply take time, effort, and a lot of mulling and reflection that, frustatingly, seem to lead nowhere at first. But every now and then you will come back to a text later, on a second reading or when considering a new example, and then discover exactly what was not yet clear before. Each such event is a small triumph and a joy, and in this way your understanding and knowledge will

gradually grow.

The structure of these notes

The nomenclature in these notes is as follows: We use the term "Proposition" for results that are relatively direct or somewhat less relevant. The name "Lemma" is used for a result that is not quite itself a main theorem, but that provide essential tools on the way to greater results. As usual, a "Theorem" is exactly such a result to remember.

As was mentioned above, one can develop a solid grasp of Galois theory without fully understanding every single proof or example. More complicated or technical information, as well as other optional results that can safely be omitted on a first reading (or indeed on all readings), has been marked* with an asterisk. Occasionally, this is the case for difficult proofs themselves; do not torture yourself by trying to learn these by heart, as this is not the point of either algebra or of mathematics in general. You can therefore safely skip all marked* parts of these notes, as well as the more fine-grained detail that is relegated to the remarks. This is especially relevant when summarizing the material or preparing for the examination.

That said, reading the additional material will broaden your view and your mathematical knowledge. It might even be fun.

Further sources

Some alternative sources that complement these rather expanded and elaborate notes now follow. The classic streamlined exposition of Galois theory can be found in Artin's book [Art98]. Another compact and extremely well-written set of notes that are more concretely oriented are those by Milne [Mil22]. Finally, Lenstra and Stevenhagen have given a highly enjoyable historical exposition on Chebotaryov's theorem in [SL96]. The latter article also gives an elegant introduction to class field theory; for more on this topic, see [LS00] and especially [Neu13].

Apart from the Langlands program, the largest single generalization of Galois theory is Grothendieck's *Long March* [Gro95], a further elaboration of the first part of his seminar on algebraic geometry [GR]. However, this material is not for the faint of heart. Lenstra's treatise [Len] presents Grothendieck's profound ideas in an extremely insightful fashion.

Acknowledgments

An attempt was made to make these notes comprehensible, concrete, and captivating. Whether or not the actual matches the potential in this regard, I am deeply grateful to those who provided feedback, criticism, and suggestions for improvement. Despite my inevitable garbling and mauling of them, they have at least pointed my nose and these notes in the right direction. Heartfealt thanks go to Tim Evink and Robert Nowak.

Chapter I

Normal extensions

In our basic algebra course, we have seen how algebraic extensions of a given field K can be constructed out of polynomials $f \in K[x]$:

(i) If f is **irreducible**, then we can construct the corresponding simple extension $K[x]/(f)$, which is generated over K by the canonical coset $\beta = x + (f)$. This extension of K is often also called the STEM FIELD of the irreducible polynomial f.

(ii) We can also construct the SPLITTING FIELD of f over K. This is an extension L of K such that we can write

$$f = (x - \beta_1) \cdots (x - \beta_n) \in L[x], \tag{1}$$

and such that $L = K(\beta_1, \ldots, \beta_n)$. If you believe in the existence of an algebraic closure $\overline{K}$ of K, then you can construct L by adjoining the zeros of f in $\overline{K}$ to K. However, the notion of a splitting field is sufficiently flexible so as not to depend on the existence of an algebraic closure (which requires Zorn's Lemma in general). Neither does the polynomial f have to be irreducible as an element of $K[x]$ for its splitting field to exist.

We have seen that given an irreducible polynomial $f \in K[x]$, both its stem field and its splitting field are uniquely determined up to isomorphism. In the first two chapters of these notes, we consider the more intricate properties of these and more general algebraic extensions in some more detail. In this chapter, we start with the notion of normality, for which we now give a down-to-earth motivation.

Let $L|K$ be an arbitrary algebraic field extension, and let $\beta \in L$, with minimal polynomial f. The theory of simple extensions relates the stem field of f with the field generated over K by β, in that it provides a K-isomorphism

$$\begin{aligned} K[x]/(f) &\xrightarrow{\sim} K(\beta) \subset L \\ x + (f) &\mapsto \beta. \end{aligned} \tag{2}$$

Suppose that $\beta' \in L$ is another zero of f. Then the minimal polynomial of β' divides f, so that it in fact equals f. We therefore also obtain a K-isomorphism

$$\begin{aligned} K[x]/(f) &\xrightarrow{\sim} K(\beta') \subset L \\ x + (f) &\mapsto \beta'. \end{aligned} \tag{3}$$

We therefore conclude that there also exists an isomorphism $K(\beta) \simeq K(\beta')$. However, our argument does not show that $K(\beta) = K(\beta')$ as subfields of L, and indeed it can happen that

$$K(\beta) \simeq K(\beta') \qquad \textbf{but} \qquad K(\beta) \neq K(\beta'). \tag{4}$$

Some of you may already have encountered this phenomenon; here is a concrete example of it. Consider the extension $L = \mathbb{C}$ of the base field $K = \mathbb{Q}$, and let $\beta = \sqrt[3]{2}$. Then the minimal polynomial of β over $\mathbb{Q}$ is given by $f = x^3 - 2$, for example since f is a cubic polynomial without zeros in $\mathbb{Q}$. We accordingly obtain an isomorphism

$$\begin{aligned} \mathbb{Q}[x]/(x^3 - 2) &\xrightarrow{\sim} \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C} \\ x + (x^3 - 2) &\mapsto \beta = \sqrt[3]{2}. \end{aligned} \tag{5}$$

In the field of complex numbers, the polynomial f has more zeros than just $\beta = \sqrt[3]{2}$. In fact the other two zeros are given by $\zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$, where ζ_3 is the primitive third zero of unity $e^{2\pi i/3}$. If we let $\beta' = \zeta_3 \sqrt[3]{2}$, then the argumentation above show the existence of another isomorphism

$$\begin{aligned} \mathbb{Q}[x]/(x^3 - 2) &\xrightarrow{\sim} \mathbb{Q}(\beta') = \mathbb{Q}(\zeta_3 \sqrt[3]{2}) \subset \mathbb{C} \\ x + (x^3 - 2) &\mapsto \beta' = \zeta_3 \sqrt[3]{2}. \end{aligned} \tag{6}$$

Now since $\mathbb{Q} \subset \mathbb{R}$ and $\beta = \sqrt[3]{2} \in \mathbb{R}$, we have that $\mathbb{Q}(\beta) \subset \mathbb{R}$, since after all $\mathbb{Q}(\beta)$ is the smallest subfield of $\mathbb{C}$ that contains both $\mathbb{Q}$ and β. On the other hand, $\mathbb{Q}(\beta')$ is not contained in $\mathbb{R}$, since $\beta' = \zeta_3 \sqrt[3]{2} \notin \mathbb{R}$. Therefore in this case we have $\mathbb{Q}(\beta) \neq \mathbb{Q}(\beta')$, even though these subfields of $\mathbb{C}$ are isomorphic as abstract field extensions of $\mathbb{Q}$.

This problem, and its more general version (4), are not at all a silly issues, and the difference between equality and isomorphism involves deep mathematics, the systematic development of which leads to category theory and stacks. In the current concrete context, it is most of all an annoyance: We cannot "point at" the field $\mathbb{Q}[x]/(x^3 - 2)$ as a subextension of $\mathbb{C}|\mathbb{Q}$, since there are in fact three possibilities to embed it into $\mathbb{C}$, namely as $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt[3]{2})$, as $\mathbb{Q}(\beta') = \mathbb{Q}(\zeta_3 \sqrt[3]{2})$, and finally as $\mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$.

This leads to the following questions:

(i) Are there conditions on a non-constant polynomial $f \in K[x]$ that guarantee that for any two zeros β and β' of f in another extension $M|K$ we always have an actual actuality $K(\beta) = K(\beta')$ as subfields of M, instead of merely a K-isomorphism?

(ii) More generally, let $L|K$ be a field extension. What condition on L guarantees that any two K-homomorphisms from L into another extension $M|K$ always have the same image in M?

To find the answer these questions, let us look at an example where the problem above does not occur. Let us consider the extension $L|K$ with $L = \mathbb{C}$ and $K = \mathbb{Q}$, and let us take the element $\beta = \sqrt{2} \in L$. This time the minimal polynomial $f = x^2 - 2 \in \mathbb{Q}[x]$ of β over $\mathbb{Q}$ has the two zeros $\pm\sqrt{2}$ in $\mathbb{C}$. Since these zeros are the negatives of one another, any field that contains one of them contains the other, so that in particular

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}). \tag{7}$$

The reason for this behavior is that once we adjoin one of the zeros of $f = x^2 - 2$, we get the other "for free". In turn, this happens because the polynomial $f = (x - \sqrt{2})(x + \sqrt{2})$ splits into linear factors over either of the fields obtained by adjoining one of its zeros. This leads to a "symmetry" among the zeros of f that resolves the issue under consideration; while the two resulting embeddings

$$\begin{aligned} \mathbb{Q}[x]/(x^2 - 2) &\to \mathbb{C} \\ x + (x^2 - 2) &\mapsto \pm\sqrt{2} \end{aligned} \tag{8}$$

are not themselves identical, their images $\mathbb{Q}(\pm\sqrt{2})$ are, because both of them already contain all zeros of f in $\mathbb{C}$. Given a more general field extension $L|K$, we can ensure the same behavior by demanding that every minimal polynomial of an element $\beta \in L$, that is, every irreducible polynomial in $K[x]$ that admits some zero in L, in fact splits into linear factors in $L[x]$. This is the notion of a NORMAL extension that is formalized in Definition 1.1. Normality is one of the conditions that Galois extensions, which we shall define in Chapter IV, have to satisfy.

After exploring the notion of normality in this chapter, we will show that it is in fact not that new; any normal field extension of M that is finitely generated over K is in fact the splitting field of some polynomial in $K[x]$. Phrased differently, an extension $L|K$ is a splitting field of a polynomial in $K[x]$ if and only if the following conditions hold:

(SF1) $L|K$ is finitely generated over K; and

(SF2) $L|K$ is a normal extenion, in the sense that **every** irreducible polynomial in $K[x]$ that admits a zero in L can be written as a product of linear factors in $L[x]$.

It may then seem that we have merely rewritten the familiar notion of a splitting field in a more pretentious way. Instead, the normality condition (SF2) illustrates an important principle. As originally defined, the notion of a splitting field always involves reference to some distinguished polynomial chosen at the start, namely the very polynomial of which it is the splitting field. When considered in this way, the property of being a splitting field is somewhat extrinsic to a field extension. However, the characterization of splitting fields by

means of (SF1) and (SF2) enables us to check whether a given extension $M|K$ is a splitting field without reference to any special polynomial because of the universal quantifier in (SF2).

We therefore see that our results in some sense do away with the arbitrary initial choice of a polynomial, and provide a more intrinsic version of the notion of a splitting field. This principle adds flexibility to our study of fields. We will also apply it when studying separable extensions and their defining polynomials in the next chapter.

1 Splitting fields as normal extensions

Our goal in this section is to find a criterion on an algebraic field extension $L|K$ that avoids the problem (4) for elements β and β' of L. As the introduction to this chapter shows, this problem is essentially caused by the fact that different zeros of a polynomial $f \in K[x]$ will generate different subfields of L in general.

As we have seen, one way to avoid this asymmetry is to insist that when $f \in K[x]$ is the minimal polynomial of an element of L, then **all** its zeros belong to L. Formalizing this notion without reference to specific elements of L, we obtain the following definition.

Definition 1.1. An algebraic field extension $L \mid K$ is called NORMAL if any irreducible polynomial $g \in K[x]$ that admits a zero in L SPLITS INTO LINEAR FACTORS in $L[x]$, in the sense that g can be written as a product of linear factors in $L[x]$.

Remark 1.2. The notion of being normal can be extended verbatim to field extensions that are not necessarily algebraic. However, in these notes, we are mainly interested in algebraic extensions. This is not only to keep our eyes on the prize; Remark 1.12(iii) will show that Theorem 1.10, the result that motivates Definition 1.1, does not generalize to the non-algebraic case.

Example 1.3. (i) Any quadratic extension $L|K$ is normal. Indeed, let $f \in K[x]$ be irreducible, and suppose that f has a zero $\beta \in L$. As f is irreducible, it is a scalar multiple of the minimal polynomial of β. The theory of simple extensions then implies that we have $\deg(f) = [K(\beta) : K]$. Since $K(\beta)|K$ is a subextension of the quadratic extension $L|K$, the tower law shows that $\deg(f) \leq 2$.

Now if $\deg(f) = 1$, then f is already itself linear. Otherwise division with remainder yields a factorization $f = (x - \beta)q$. The multiplicativity of the degree then shows that $\deg(q) = \deg(f) - \deg((x - \beta)) = 2 - 1 = 1$. Therefore f splits into linear factors in this case as well. Since f was arbitrary, we have shown that $L|K$ is indeed normal.

(ii) The discussion in the introduction shows that the field extension $L = \mathbb{Q}(\sqrt[3]{2})$ of $K = \mathbb{Q}$, which is isomorphic to the stem field over $\mathbb{Q}$ of the irreducible polynomial $f = x^3 - 2$, is not normal. Indeed, the field $L \subset \mathbb{R}$ contains only one of the three distinct zeros of the polynomial f in $\mathbb{C}$, and in

particular does not split over $L[x]$; instead its factorization into irreducible polynomials in $L[x]$ is given by

$$f = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}). \tag{9}$$

In comparison with Part (i), the non-normality in this new example comes from the fact that this time to complementary factor to $x - \beta = x - \sqrt[3]{2}$ does not split into linear factors.

Though the stem field of the irreducible cubic polynomial f in this example is not normal, Theorem 1.6 will show that its splitting field still is. Moreover, in Example 1.9(ii) we will see an example of a cubic number field that is normal.

(iii) If $\overline{K}$ is the algebraic closure of a given field K, then the very definition of the algebraic closure implies that the field extension $\overline{K}|K$ is normal. ❀

Splitting fields provide an important class of normal extensions. To show this, we recall the prolongation lemma:

Lemma 1.4. *Let K be a field, let $f \in K[x]$ be a non-zero univariate polynomial. Let $L|K$ be a field extension generated by zeros of the polynomial f, and let $L'|K$ be a field extension over which f splits into linear factors. Let $M|K$ (respectively $M'|K$) be a subextension of $L|K$ (respectively $L'|K$), and suppose that a K-homomorphism*

$$\varphi : M \to M' \tag{10}$$

is given. Then there exists a K-homomorphism

$$\psi : L \to L' \tag{11}$$

such that $\psi|_M = \varphi$.

We also state a useful principle that we have used multiple times when discussing the elementary theory of fields.

Proposition 1.5. *Let $L|K$ and $L'|K$ be field extensions, and let $\varphi : L \to L'$ be a K-homomorphism. If $\beta \in L$ is such that $f(\beta) = 0$ for $f \in K[x]$, then also $f(\sigma(\beta)) = 0$.*

We can now show the desired result on splitting fields.

Theorem 1.6. *Let K be a field, let $f \in K[x]$ be a non-zero univariate polynomial, and let L be a splitting field of f. Then the algebraic extension $L|K$ is normal.*

Proof. Let $g \in K[x]$ be an irreducible polynomial that admits a zero in L, say γ. We have to show that g splits into linear factors in $L[x]$. For this, we may assume that f and g are monic, and we then first construct a splitting field M over K of the product polynomial $fg \in K[x]$. Over this field, the polynomials f and g both split into linear factors, say as the powers

$$f = (x - \beta_1)^{r_1} \cdots (x - \beta_n)^{r_n} \tag{12}$$

and

$$g = (x-\gamma_1)^{s_1}\cdots(x-\gamma_m)^{s_m} \tag{13}$$

of pairwise distinct linear polynomials. It now suffices to show that if γ' is a second zero of g in M, then γ' actually belongs to L, considered as the subfield $K(\beta_1,\dots,\beta_n)$ of M.

Since g is irreducible over K, both simple field extensions $K(\gamma)$ and $K(\gamma')$ are isomorphic to the stem field $K[x]/(g)$. More precisely, there exists a K-isomorphism

$$\begin{aligned} \varphi : K(\gamma) &\xrightarrow{\sim} K(\gamma') \\ \gamma &\to \gamma'. \end{aligned} \tag{14}$$

Lemma 1.4 implies that we can prolong φ to a K-automorphism $\sigma : M \to M$ of the splitting field M. In particular, we have

$$\sigma(\gamma) = \varphi(\gamma) = \gamma'. \tag{15}$$

As γ belongs to L, we conclude that to show that $\gamma' \in L$, it is enough to show that σ maps L to L. But this is certainly the case, as the automorphisms of σ maps the set of zeros $\{\beta_1,\dots,\beta_n\}$ of f to itself by Proposition 1.5. Therefore σ also maps the field $L = K(\beta_1,\dots,\beta_n)$ generated by these zeros to itself. This proves our claim on σ, and with it, the theorem. ♡

Remark 1.7. (i) The idea behind the statement of Theorem 1.6 is in line with our motivation in the introduction to this chapter; the splitting field of a polynomial $f \in K[x]$ should be normal since it is symmetric, in the sense that it is generated by the **full** set of zeros of f. What makes the proof complicated is that Definition 1.1 requires us to check that **all** irreducible polynomials g in $K[x]$ that admit a zero in L, and not merely the irreducible factors of the particular polynomial f, split into linear factors in L. This is the reason why we consider the auxiliary splitting field M of fg in the proof of Theorem 1.6. It will also play a role in the proof of Theorem 1.10.

(ii) While Theorem 1.6 is conceptually very pleasing, we have not quite made the factorization of g constructive, as it involves the rather opaque prolongation lemma 1.4. In Corollary III.2.5, we shall see how the factorization of g can be made explicit for the slightly more special case of finite Galois extensions $L|K$. ❁

Corollary 1.8. *Let $L|K$ be a field extension with L and K finite. Then $L|K$ is normal.*

Proof. This follows from Theorem 1.6 since every finite field is a splitting field. Indeed, if L has q elements, then it is the splitting field of the polynomial $x^q - x$ over K. ♡

Example 1.9. (i) Consider $f = x^3 - 2$ as a polynomial over the finite field $\mathbb{F}_7$. Then f is irreducible in $\mathbb{F}_7[x]$, since it is of degree 3 and does not have any zero in $\mathbb{F}_7$. We thus obtain a cubic stem field $K = \mathbb{F}_7[x]/(f)$.

The field $K \simeq \mathbb{F}_{7^3}$ is normal by Corollary 1.8, so that in particular the polynomial f splits into linear factors over K. In fact, if we let $\alpha = x + (f)$,

then because $1^3 = 2^3 = 4^3 = 1$ modulo 7 we have that the three distinct elements α, 2α and 4α are all zeros of f, since

$$2 = \alpha^3 = 2^3\alpha^3 = (2\alpha)^3 = 4^3\alpha^3 = (4\alpha)^3. \tag{16}$$

Unique factorization in polynomial rings over fields therefore implies that

$$f = (x-\alpha)(x-2\alpha)(x-4\alpha) \in K[x]. \tag{17}$$

(ii) The polynomial $f = x^3 - x^2 - 2x + 1 \in \mathbb{Q}[x]$ can be shown to be irreducible. Let $K = \mathbb{Q}[x]/(f)$ be the corresponding stem field. Then by construction f admits the zero $\alpha = x + (f)$ in K. This is not the only such zero, as in fact

$$f = (x-\alpha)(x+\alpha^2-2)(x-\alpha^2+\alpha+1) \in K[x]. \tag{18}$$

There are multiple ways to prove (18). Besides a direct verification by using the defining relations in K, one can also use the matrix representation

$$M_\alpha = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 2 \\ 0 & -1 & 1 \end{pmatrix} \in M_{3,3}(\mathbb{Q}) \tag{19}$$

of the multiplication map by α with respect to the $\mathbb{Q}$-basis $(1, \alpha, \alpha^2)$ of K. One calculates that

$$M_{-\alpha^2+2} = -M_\alpha^2 + 2 = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix} \in M_{3,3}(\mathbb{Q}) \tag{20}$$

and

$$M_{\alpha^2-\alpha-1} = M_\alpha^2 - M_\alpha - 1 = \begin{pmatrix} -1 & -1 & 0 \\ -1 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix} \in M_{3,3}(\mathbb{Q}). \tag{21}$$

The characteristic polynomials of the two matrices in (20) and (21) both equal f. The Cayley–Hamilton theorem then implies that multiplication by the elements $f(-\alpha^2+2)$ and $f(\alpha^2-\alpha-1)$ induces the zero map on K, so that α^2+2 and $\alpha^2-\alpha-1$ are indeed zeros of f, proving (18).

The existence of the factorization (18) is important because it implies that $K = \mathbb{Q}[x]/(f) = \mathbb{Q}(\alpha)$ already contains all zeros of f. It is therefore the splitting field of f, and therefore a normal extension of $\mathbb{Q}$ by Theorem 1.6. This example serves as a contrast to the cubic polynomial considered in Example 1.3(i), which did not define a normal extension of $\mathbb{Q}$.

(iii) Note that it is far from obvious how to find the factorization (18), and for that matter, how to prove that this polynomial f is irreducible over $\mathbb{Q}$. We will gloss over these issues in what follows, and refer to a course on algorithmic algebra for a fuller consideration of this theme. ❀

We now show that the concept of a normal field extension is "right", as it is the exact condition that catches the answers to Question (i) and (ii) from the introduction to this chapter. The upcoming theorem considers Question (ii). Do not sweat the details of its proof; it is its statement that counts.

Theorem 1.10. *Let $L|K$ be an algebraic field extension. Then the following statements are equivalent.*

(i) The extension $L|K$ is normal.

(ii) If $M \mid K$ is any other field extension of K, and φ and φ' are any two K-homomorphisms from L into M, then $\varphi(L) = \varphi'(L)$.

*Proof**. Suppose first that (i) holds, and let M and φ, φ' as in (ii) be given. Let $\gamma \in M$ be an element of the form $\varphi(\beta)$ with $\beta \in L$. Since L is algebraic over K, the same is true for β. Let $g \in K[x]$ be its minimal polynomial. Then g admits the zero β in L, and therefore by our hypothesis (i) we see that g splits into linear factors over L, say as

$$g = (x - \beta_1)^{r_1} \cdots (x - \beta_n)^{r_n} \in L[x]. \tag{22}$$

Applying φ to both sides of (22), we obtain

$$g = \varphi(g) = (x - \varphi(\beta_1))^{r_1} \cdots (x - \varphi(\beta_n))^{r_n} \in M[x] \tag{23}$$

and similarly for φ', so that in fact

$$K(\varphi(\beta_1), \ldots, \varphi(\beta_n)) = K(\varphi'(\beta_1), \ldots, \varphi'(\beta_n)), \tag{24}$$

as both fields in (24) are the field obtained by adjoining the full set of zeros of g in M to K.

Our goal is to show that γ is not only in the image of the original K-homomorphism $\varphi : L \to M$, but in the image of the other K-homomorphism $\varphi' : L \to M$ as well. It suffices to show that this is the case after replacing φ' by its restriction

$$\begin{aligned} K(\beta_1, \ldots, \beta_n) &\to K(\varphi'(\beta_1), \ldots, \varphi'(\beta_n)) \\ \beta_i &\mapsto \varphi'(\beta_i), \end{aligned} \tag{25}$$

which by the above considerations is an isomorphism that by abuse of notation we shall again denote by φ'. Now by Proposition 1.5 the element $\gamma = \varphi(\beta)$ is one of the zeros $\varphi(\beta_1), \ldots, \varphi(\beta_n)$ of g in $K(\varphi(\beta_1), \ldots, \varphi(\beta_n))$. It is therefore equally well one of the zeros $\varphi'(\beta_1), \ldots, \varphi'(\beta_n)$ of g in $K(\varphi'(\beta_1), \ldots, \varphi'(\beta_n))$, which after all coincides with the former field by (24). This implies that there exists some β' among the $\beta_1, \ldots, \beta_n$ such that $\varphi'(\beta') = \gamma = \varphi(\beta)$. This is exactly what we wanted to show.

Now suppose that (ii) holds. We first suppose that the algebraic extension $L|K$ is finitely generated, say $L = K(\beta_1, \ldots, \beta_n)$. Let $g \in K[x]$ be an irreducible polynomial that admits a zero β in L. Our intention is to show that g splits into linear factors over L. To this end, we define f_i to be the minimal polynomial of β_i for $1 \le i \le n$, and we let M be the splitting field of the polynomial $f_1 \cdots f_n g$. The prolongation lemma 1.4 shows that there exists an inclusion homomorphism $\varphi : L \to M$.

The polynomial g splits into linear factors over the splitting field M. In order to show that g splits into linear factors over L, it therefore suffices to show that if β' is any other zero of g in M, then β' in fact already belongs to the image $\varphi(L)$ of L in M. Now as in the proof of Theorem 1.6, we see that there exists a

K-automorphism $\sigma : M \to M$ such that $\sigma(\beta) = \beta'$. The statement (i) therefore follows if we can show that σ maps $\varphi(L)$ to itself. But this indeed has to do, as φ and $\sigma\varphi$ are two K-homomorphisms of L into M, so that by our hypothesis (i) we obtain

$$\sigma(\varphi(L)) = (\sigma\varphi)(L) = \varphi(L). \tag{26}$$

It remains to consider the case where the extension $L \mid K$ is not finitely generated. We only sketch this part of the proof, as it is merely a more involved version of what precedes it. Choose an algebraic closure $\overline{K}$ of K. An application of Zorn's Lemma shows that there exists a K-homomorphism from L into $\overline{K}$; see Exercise 1. Let us consider L as a subfield of $\overline{K}$ by means of any such embedding, and let $g \in K[x]$ be an irreducible polynomial that admits a zero β in L. If β' is another zero of g in $\overline{K}$, then yet another application of Zorn's lemma (see Exercise 2) shows that the K-homomorphism

$$\begin{aligned} K(\beta) &\xrightarrow{\sim} K(\beta') \to \overline{K} \\ \beta &\mapsto \beta' \end{aligned} \tag{27}$$

extends to a K-homomorphism $\sigma : \overline{K} \to \overline{K}$ (which is in fact a K-automorphism; see Exercise 3). As above, we see that the σ maps L to itself, and that this implies that g splits into linear factors over L. Since $g \in K[x]$ was an arbitrary irreducible polynomial, we have again shown (i). ♡

Example 1.11. In light of Theorem 1.10, Example 1.9(ii) implies that all embeddings of the field $K = \mathbb{Q}[x]/(x^3 - x^2 - 2x + 1)$ into $\mathbb{C}$ have the same image. Said image can be described as $\mathbb{Q}(\alpha)$, where α is any of the three zeros of α in $\mathbb{C}$. Note that these zeros all belong to $\mathbb{R}$. Indeed, since $x^3 - x^2 - 2x + 1$ is a cubic polynomial, it admits at least one zero in $\mathbb{R}$, and since this real zero generates the image of any embedding of K into $\mathbb{C}$, the other zeros of f in $\mathbb{C}$ have to be real as well. We again note how the normality of the extension K of $\mathbb{Q}$ yields symmetric and uniform behavior of the zeros of f in $\mathbb{C}$.

By contrast, we have already seen in the introduction to this chapter that the embeddings of the non-normal extension $K = \mathbb{Q}[x]/(x^3 - 2)$ of $\mathbb{Q}$ into $\mathbb{C}$ give rise to three possible images. Exactly one of these images is contained in $\mathbb{R}$, namely that generated by the zero $\sqrt[3]{2}$ of f. ❀

Remark 1.12. (i) It suffices to take M to be the algebraic closure $\overline{K}$ in Theorem 1.10(i); see Exercise 4.

(ii) In the statement of Theorem 1.10, the extension $M \mid K$ need not be algebraic. Note that as $L \mid K$ is algebraic, the image of both φ and φ' will be contained in the algebraic closure of K inside M anyway.

(iii) Despite Part (ii) of this remark, the hypothesis that $L \mid K$ be algebraic is still essential to obtain Theorem 1.10. For example, let $L = \mathbb{Q}(x)$ be the rational function field over $K = \mathbb{Q}$. Then $L \mid K$ is a normal extension in the sense of Remark 1.2(ii). However, we can embed L into itself both by sending x to x and by sending x to x^2, and whereas the former embedding has L itself as its image, the image of the latter equals the proper subextension $\mathbb{Q}(x^2)$ of L. ❁

Specializing Theorem 1.10 to simple extensions, we obtain the answer to Question (i) in the introduction, which can be considered as a generalization of the idea in Example 1.3(i). We only consider the case where $f \in K[x]$ is irreducible and $L = \overline{K}$; see Exercises 5 and 6 for more general statements.

Corollary 1.13. *Let K be a field with algebraic closure $\overline{K}$, and let $f \in K[x]$ be an irreducible polynomial. Then the following statements are equivalent.*

(i) The stem field $K[x]/(f)$ is a normal extension of K.

(ii) The polynomial f splits into linear factors over its stem field $K[x]/(f)$.

(iii) For any extension $M|K$ and for any two zeros β and β' of f in M we have $K(\beta) = K(\beta')$.

Proof. (i) $\Leftrightarrow$ (ii): If $L|K$ is normal, then in particular the polynomial f splits into linear factors over it, since it is irreducible over K and admits the canonical zero $x + (f)$ in L. Conversely, if f splits into linear factors over L, then L is a splitting field of f, since it is generated by $x + (f)$ over K and f splits into linear factors over it. Theorem 1.6 then shows that $L|K$ is normal.

(ii) $\Leftrightarrow$ (iii): By the theory of simple extensions, the fields $K(\beta)$ in M generated by the various zeros β of f in M are nothing but the images of the various K-homomorphisms from the stem field $L = K[x]/(f)$ into M. The proof of Theorem 1.10 shows that these images all coincide if and only if $L|K$ is a normal extension. ♡

Remark 1.14. Note how the statement of Theorem 1.10, which is formulated for fields, is somewhat more elegant than Corollary 1.13, which considers a distinguished polynomial. However, the criteria from Corollary 1.13 reduce checking normality to a finite computation, which is not the case for the universal statement in Theorem 1.10.

These results are actually different aspects of a recurring phenomenon in field theory, a philosophy or yoga if you will. Often, a notion, be it algebraicity, normality, or (as in the next chapter) separability is first defined on the level of elements or polynomials, but then generalized to the context of fields, typically by means of the universal quantifier, as in Theorem 1.10. The subtlety is then usually to show that given a field extension $L|K$, the property in question can be verified in practice by means of a chosen set of generators of $L|K$. Corollary 1.13 is an incarnation of this principle; for a more general result, see Exercise 7. ❁

2 Normal extensions as splitting fields

Given a base field K, Theorem 1.6 shows that the splitting fields of polynomials $f \in K[x]$ yield normal extensions of K. In fact, we can now prove the criterion in the introduction to this chapter, which shows that when we restrict our attention to normal algebraic extensions that are moreover finitely generated, then splitting fields are all that we get.

Theorem 2.1. *Let $L|K$ be a field extension of finite degree. Then $L|K$ is normal if and only if it is the splitting field of a polynomial $f \in K[x]$.*

Proof. If $L|K$ is a splitting field, then it is normal by Theorem 1.6. It therefore suffices to prove the converse implication.

Since $L|K$ is finite, we have $L = K(\beta_1, \dots, \beta_n)$ for elements $\beta_i \in L$ with minimal polynomial $f_i \in K[x]$ say. Since $L|K$ is normal, it contains all the zeros of the polynomials f_i. It therefore contains the splitting field of the product polynomial $f = f_1 \cdots f_n \in K[x]$. As conversely $L|K$ is generated by a subset of these zeros, we see that $L|K$ is the splitting field of f over K. ♡

Remark 2.2. (i) The primitive element theorem implies that we can in practice often even take the polynomial $f \in K[x]$ from Theorem 2.1 to be irreducible, but as we shall see in Example II.2.13(ii), there are some finicky exceptions to this principle; also see Remark 4.2(i).

(ii) The finiteness hypothesis in Theorem 2.1 is essential, as any extension obtained as the splitting field of a polynomial is of necessity finite. In particular, the algebraic extension $\overline{\mathbb{Q}}|\mathbb{Q}$ may be normal by Example 1.3(iii), but it is not a splitting field. However, Exercise 8 implies that this extension, and in fact any normal algebraic extension, can be obtained as the splitting field of a (possibly infinite) **family** of polynomials. ❁

Remark 2.3. One of the texts to formalize to concept of a normal extension was the 1981 book Éléments de Mathématiques written by Nicolas Bourbaki, who did not actually exist. This statement requires some explanation.[1]

Shortly before the Second World War, a number of French mathematicians met to write a series of textbooks on modern mathematics. Because of the casualties in the First World War, such resources were severely lacking at the time. (André Weil blamed these high casualties among scientists on French egalitarianism and was of the opinion that Germany had been more protective of its young scientists.) The group signed their works with the last name of the unfortunate French general Charles-Denis Bourbaki, who was fairly well-known at the time. The brand new first name was suggested by Eveline de Possel, the wife of one of the group members. Incidentally, to these days the French expression "armée de Bourbaki" means a rag-tag and ill-equipped group of people — make of that what you will.

Bourbaki's work had a profound influence on mathematics. The very fact that a group of mathematicians could work together so intensively, profoundly, and consistently for such a long time is already exceptional in itself. Moreover, their abstract point of view was highly successful, and suffused most of mathematics in the second part of the twentieth century. On the other hand, the Bourbaki style is often overly abstract and top-down; concrete examples are only rarely present in their texts, which therefore basically assume that their readers already know what they are about. This aversion towards any kind of hands-on approach led to the failure of the New Math, a mathematical-didactic paradigm inspired by Bourbaki's methods.

In Bourbaki's language, a normal extension is called a quasi-Galois extension. The reason for this is that normal extensions (and splitting fields)

[1] For more of it, see https://en.wikipedia.org/wiki/Nicolas_Bourbaki [Accessed 16 May 2024]

are "essentially" Galois extensions, except for the final technical condition of separability that we discuss in the next chapter. There exists a generalization of Galois theory to the broader context of normal field extensions; it is called the Jacobson–Bourbaki theorem. Note that Nathan Jacobson (1910–1999) did actually exist. ❁

3 Exercises for Chapter I

Exercise 1. Let $L|K$ be an algebraic field extension and let $\overline{K}$ be an algebraic closure of L. Let S be the set of pairs (M,φ), where M is a subextension of $L|K$ and where $\varphi : M \to \overline{K}$ is a K-morphism. We make S into a partially ordered set by decreeing that $(M,\varphi) \leq (M',\varphi')$ if and only if $M \subset M'$ and the restriction of φ' to M equals φ.

(i) Show that every chain in S has an upper bound.

(ii) Use Zorn's lemma to conclude that S has a maximal element (N,ψ).

(iii) Use the prolongation lemma 1.4 to show that $N = L$ and conclude that L admits a K-homomorphism into $\overline{K}$.

Exercise 2. Generalize the method from Exercise 1 to prove that if $\beta \in L$, then any K-homomorphism $K(\beta) \to \overline{K}$ extends to a K-homomorphism $L \to \overline{K}$.

Exercise 3. Show that the K-homomorphism $\sigma : \overline{K} \to \overline{K}$ from (27) is in fact a K-automorphism. More generally, show that any K-homomorphism $\sigma : L \to L$ from an algebraic extension $L|K$ to itself is in fact a K-automorphism.

Exercise 4. Show that the conditions in Theorem 1.10 are equivalent to the following:

(ii') If φ and φ' are any two K-homomorphisms from L into $\overline{K}$, then $\varphi(L) = \varphi'(L)$.

Exercise 5. Show that the statements in Corollary 1.13 are equivalent to the following:

(iii') For any two zeros β and β' of f in $\overline{K}$ we have $K(\beta) = K(\beta')$.

Exercise 6. Prove the following generalization of Corollary 1.13: Let $f \in K[x]$ be a non-zero polynomial, not necessarily irreducible. Then the following statements are equivalent.

(i) For any extension $M|K$ and for any two zeros β and β' of f in M we have $K(\beta) = K(\beta')$.

(ii) The polynomial f is a product of irreducible polynomials $g_1 \cdots g_r$ whose stem fields are isomorphic normal extensions of K.

Exercise 7. Let $L = K(\beta_1,\ldots,\beta_n)$ be a finitely generated algebraic extension. Show that the following statements are equivalent.

(i) $L|K$ is normal.

(ii) The minimal polynomials of the elements $\beta_1,\dots,\beta_n$ split into linear factors in $L[x]$.

Exercise 8. Let $L|K$ be an algebraic field extension. Show that the following statements are equivalent.

(i) $L|K$ is normal.

(ii) There exists a (possibly infinite) family $(\beta_i)_{i\in I}$ of elements of L such that $L = K((\beta_i)_{i\in I})$, and moreover all minimal polynomials of the elements β_i split into linear factors over L.

(iii) L is the splitting field of a (possibly infinite) family of polynomials $(f_i)_{i\in I}$ in $K[x]$, in the sense that all f_i split into linear factors over L and that L is generated over K by the zeros of these polynomials.

Exercise 9. For each of the following pairs K and f, determine whether the stem field over K determined by the irreducible polynomial $f \in K[x]$ is normal or not.

(i) $K = \mathbb{Q}$, $f = x^2 + 17$.

(ii) $K = \mathbb{Q}$, $f = x^4 - 2$.

(iii) $K = \mathbb{Q}(\sqrt{-1})$, $f = x^4 - 2$.

(iv) $K = \mathbb{Q}$, $f = x^3 - 3x - 1$.

(v) $K = \mathbb{Q}$, $f = x^3 + 3x - 1$.

(vi) $K = \mathbb{F}_7$, $f = x^3 - 3x - 1$.

(vii) $K = \mathbb{F}_{17}$, $f = x^3 + 3x - 1$

Exercise 10. Find an irreducible quartic polynomial $f \in \mathbb{Q}[x]$ such that the stem field $K = \mathbb{Q}[x]/(x^4 - 2)$ admits 4 embeddings $\varphi_i : K \to \mathbb{C}$ such that

$$\varphi_1(K) = \varphi_2(K) \neq \varphi_3(K) = \varphi_4(K).$$

Exercise 11. Let $M|K$ be a subextension of a normal algebraic extension $L|K$.

(i) Show that $L|M$ is again a normal extension.

(ii) Show that $M|K$ need not be a normal extension.

Exercise 12. Let $L|K$ be a finite extension of fields. Choose elements $\beta_1,\dots,\beta_n$ of L such that $L = K(\beta_1,\dots,\beta_n)$, and for all i between 1 and n, define f_i to be the minimal polynomial of β_i. Finally, let $f = f_1 \cdots f_n \in K[x]$ and define N to be the splitting field of f.

(i) Show that there exists a K-homomorphism $\varphi : L \to N$.

(ii) Let N' be a normal extension of K, and consider a K-homomorphism $\varphi' : L \to N'$. Show that there exists a K-homomorphism $\psi : N \to N'$ such that $\varphi' = \psi\varphi$.

The extension $N|K$ considered above is called the NORMAL CLOSURE of the extension $L|K$.

Exercise 13. We generalize the construction of the normal closure from the previous exercise. Let $L|K$ be an algebraic extension (not necessarily finite), and define

$$N = \prod_{\varphi : L \to \overline{K}} \varphi(L) := \langle \varphi(L) \,:\, \varphi : L \to \overline{K} \text{ a } K\text{-homomorphism} \rangle$$

to be the COMPOSITUM of the images of L under the various embeddings φ of L into the algebraic closure $\overline{K}$, i.e. the smallest extension of $\overline{K}|K$ that contains all these images.

(i) Show that there exists a K-homomorphism $\varphi : L \to N$.

(ii) Let N' be a normal extension of K, and consider a K-homomorphism $\varphi' : L \to N'$. Show that there exists a K-homomorphism $\psi : N \to N'$ such that $\varphi' = \psi\varphi$.

Exercise 14. For devout non-believers: State and prove all the results in this chapter without making use of an algebraic closure.

Summary and main notions of the chapter

We have solved Questions (i) and (ii) in the introduction to this chapter by introducing the notion of a normal extension (Definition 1.1). Because of our results, we can phrase the answers to these questions as follows:

(i) Provided that f be irreducible, Corollary 1.13 implies that $K(\beta) = K(\beta')$ for any two zeros β and β' of f in another field extension $M|K$ if and only if the polynomial f splits into linear factors over its stem field $K[x]/(f)$.

(ii) Provided that the extension $L|K$ be algebraic, Theorem 2.1, show that the images of K-homomorphisms of L into other extensions $M|K$ all coincide exactly if the extension $L|K$ is normal.

The key skills to take away from this are the following:

– You are able to formulate the concise condition on a field to admit essentially unique embeddings into other fields (Definition 1.1 and Theorem 1.10), and you are able to formulate this especially concretely in the particular case of stem fields (Corollary 1.13).

– You are aware of the equivalence between being normal and being a splitting field for the particular case of extensions of finite degree (Theorem 2.1).

– You can give some concrete examples of normal extensions, such as splitting fields (Theorem 1.6) and extensions of finite fields (Corollary 1.8).

Chapter II

Separable extensions

The previous chapter showed that every finitely generated normal field extension $L|K$ is in fact the splitting field of a polynomial $f \in K[x]$. Factoring this polynomial into distinct irreducibles f_i, we can write it as a product

$$f = f_1^{e_1} \cdots f_r^{e_r} \in K[x]. \tag{1}$$

Since the set of zeros of the polynomial f is exactly the union of the set of zeros of the factors $f_1, \ldots, f_r$, we may as well suppose that f admits the factorization

$$f = f_1 \cdots f_r \in K[x] \tag{2}$$

in which every factor occurs with multiplicity 1; in this case, we call f square-free. Now since the f_i are distinct irreducible polynomials, one might be tempted to conclude that because we eliminated superfluous multiplicities, the polynomial f has no repeated zeros in the algebraic closure $\overline{K}$.

Somewhat surprisingly, this suspicion is incorrect, as the following iconic counterexample shows. Suppose that $K = \mathbb{F}_q(t)$ is a rational function field over a finite field $\mathbb{F}_q$ of characteristic p say. Then we can consider the polynomial

$$f = x^p - t \in K[x]. \tag{3}$$

This polynomial is irreducible, as can be shown by applying the Eisenstein criterion for the prime element t of the ring $R = \mathbb{F}_q[t]$. Now let $L = K[x]/(x^p - t)$ be the stem field of, and let β be the canonical element $x + (x^p - t)$ of L. Then by construction $\beta^p = t$ in L, so that we will simply denote β by $t^{1/p}$ instead. Now the binomial formula in characteristic p shows that

$$f = (x - t^{1/p})^p \in L[x]. \tag{4}$$

We see that although f has no repeated factors as an element of $K[x]$, it nevertheless decomposes a power in $L[x]$. Another way to state this is by saying that the property of f being square-free is not stable under extension of the base field K to L.

As this is a strange phenomenon, we would like to understand it somewhat better. We do this by means of the following questions:

(i) Given a field K, can we classify the irreducible polynomials $f \in K[x]$ that obtain repeated zeros over an extension of K, thus showing behavior as that in (4)?

(ii) Are there any conditions on the base field K that ensure that such strange behavior **never** occurs for square-free polynomials $f \in K[x]$? In other words: For which fields K can we be sure that any square-free polynomial with coefficients in K remains square-free over any extension of K?

It will turn out that the p-th powering behavior in (4) is essentially the sole source of repeated zeros over extensions of K, and that a full classification of irreducible polynomials with repeated zeros in $\overline{K}$ can be given; see Proposition 1.5. As in the previous chapter, it will turn out to be advantageous to formulate this phenomenon not only for individual polynomials, but also for field extensions. This leads to the formal notion called INSEPARABILITY.

The good news is that problematic behavior in (4) is quite rare, in the sense that it will never occur for irreducible polynomials over finite fields or over number fields. In this sense, the notion of inseparability is often merely somewhat of a theoretical hobgoblin. Still, it is very important to be aware of this issue... especially if you intend to study function fields such as $\mathbb{F}_q(t)$, as in that context dealing with inseparability and its many consequences often requireness a certain amount of artfulness and cunning.

1 Separability for polynomials

Our goal in this section is to deal with repeated zeros of polynomials over fields. As we saw in the introduction, this may depend on the base field that is used. We need to define some decent terminology to deal with these subtleties.

Definition 1.1. Let K be a field, and let $f \in K[x]$ be a non-zero polynomial, with factorization

$$f = \alpha f_1 \cdots f_r \in K[x] \tag{5}$$

with $\alpha \in K$ and with $f_i \in K[x]$ monic and irreducible. We say that f is SQUARE-FREE if the factors f_i in (5) are pairwise distinct. Moreover, we say that f is SEPARABLE if it is square-free over any extension of K (and in particular over K itself); otherwise we say that f is INSEPARABLE. ✌

While Definition 1.1 speaks of repeated factors instead of repeated zeros, the principle in the upcoming Proposition 1.2 will allow us to reduce the study of separability of a polynomial $f \in K[x]$ to that of the zeros of f in the algebraic closure $\overline{K}$.

Proposition 1.2. *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial. Then f is separable if and only if all zeros of f in $\overline{K}$ are of multiplicity one, in the sense that we have*

$$f = \alpha(x - \beta_1) \cdots (x - \beta_n) \in \overline{K}[x] \tag{6}$$

for mutually distinct $\beta_i \in \overline{K}$ and for some $\alpha \in K$.

Proof. If f is separable, then it is necessarily square-free as a polynomial over $\overline{K}$, so that the zeros β_i of f in the factorization (6) are distinct. Conversely, if this is the case, then the same holds for the zeros of f over the splitting field $L = K(\beta_1, \ldots, \beta_n)$.

This being so, let $M \mid K$ be another extension of K; we will show that f is square-free as an element of $M[x]$. Let N be the splitting field of f considered as a polynomial in $M[x]$. Then the prolongation lemma I.1.4 implies that there exists a K-homomorphism from L into N. In particular, the factorization (6) is also a factorization of f into distinct linear factors in $N[x]$. If f were not square-free in $M[x]$, we would have $g^2 | f$ for some non-constant polynomial $g \in M[x]$, and since the chosen splitting field N of f over M contains a splitting of g over M, this would give rise to a repeated linear factor of f in $N[x]$, which it does not possess. ♡

Example 1.3. Let p be a prime number, let F be a field of characteristic p, and let $K = F(t)$ be the rational function field over F in the variable t. As in the introduction to this chapter, we see that the polynomial

$$f = x^p - t \in K[x] \tag{7}$$

is inseparable, even though it is square-free. After all, we can write

$$f = (x - t^{1/p})^p \in \overline{K}[x], \tag{8}$$

so that f admits $t^{1/p}$ as a zero with multiplicity p. ❀

There are many examples of inseparable polynomials over any given field; just choose your favorite polynomial over K (say x) and raise it to a power at least 2 to obtain an inseparable polynomial in $K[x]$. On the other hand, as irreducible polynomials fulfill a minimality condition, they are often automatically separable. The upcoming proposition is an important case of this principle.

Proposition 1.4. *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial. If f is irreducible and* $\operatorname{char}(K) = 0$, *then f is separable.*

Proof. Suppose that f were inseparable. Then f would admit repeated zero β over $\overline{K}$. Let us write

$$f = (x - \beta)^2 g, \qquad \text{with } g \in \overline{K}[x]. \tag{9}$$

Then for the derivative $f' \in K[x]$ we have

$$f'(\beta) = 2(x - \beta)g + (x - \beta^2)g' = (x - \beta)(2g + (x - \beta)g') \in \overline{K}[x]. \tag{10}$$

In particular, β is also a zero of f'. Let us write

$$f = \alpha_0 x^n + \ldots + \alpha_n \qquad \text{with } \alpha_0 \neq 0. \tag{11}$$

Then f' contains the term $n\alpha_0 x^{n-1}$. We have $\alpha_0 \neq 0$ by assumption, and moreover $n \neq 0$ by our hypothesis $\operatorname{char}(K) = 0$. Since K is a field, and therefore an integral domain, we see that $n\alpha_0 \neq 0$, so that in particular f' is not the zero polynomial.

However, this is a contradiction: Since f is irreducible, it is in fact the minimal polynomial of its zero $\beta \in \overline{K}$. Therefore f divides f', which is impossible as f' is non-zero and $\deg(f') < \deg(f)$. ♡

Over fields of prime characteristic, the situation is a bit more complicated, but we still have a fairly good grip on what happens. In particular, we can solve Question (i) from the introduction to this chapter in this context.

Proposition 1.5. *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial. If f is irreducible and $\mathrm{char}(K) = p$ is a prime number, then there exists a separable irreducible polynomial $g \in K[x]$ and a power q of p such that $f = g(x^q)$. In particular, if f is inseparable, then its degree is divisible by p.*

Proof. The proof of Proposition 1.4 shows that the irreducibility of f implies that the derivative f' is the zero polynomial in $K[x]$. If $\alpha_{n-i}x_i$ is a monomial in f, then f' contains the contribution $i\alpha_{n-i}x_{i-1}$. If i is not divisible by p, then the proof of Proposition 1.4 shows that f' is non-zero. Since this is exactly what we excluded, we conclude that f only contains monomials that are powers of x^p. This allows us to write $f = g(x^p)$ for some polynomial $g \in K[x]$.

Now g is irreducible, as any non-trivial factorization $g = h_1h_2$ would give rise to a non-trivial factorization $f = g(x^p) = h_1(x^p)h_2(x^p)$ of f. Continuing inductively and using that $\deg(f)$ is finite, we obtain the statement of the Proposition. ♡

In Propositions 1.4 and 1.5 we have used the derivative to great effect. It can in fact be used in general to decide whether a given polynomial (irreducible or not) is separable.

Proposition 1.6. *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial. Then f is separable if and only if $\gcd(f, f') = 1$, that is, if and only if $(f, f') = (1) = K[x]$.*

Proof. We first observe that given $g \in K[x]$ we have $(f, g) = (1)$ if and only if f and g have no common zero in $\overline{K}$. Indeed, if (f, g) is not all of $K[x]$, then it is generated by a non-constant polynomial $h \in K[x]$. This polynomial divides both f and g, so that any zero of h in $\overline{K}$ is a zero of both f and g. Conversely, if $(f, g) = K[x] = (1)$, then Bézout's lemma shows that we can write $1 = af + bg$ for some $a, b \in K[x]$. Any common zero of f and g would then also be a zero of 1, but that polynomial does not admit a zero in any extension of K.

We now take $g = f'$ in the previous paragraph. Proposition 1.2 implies that is enough to show that β in $\overline{K}$ is a repeated zero of f if and only if it is a common zero of f and its derivative f'. If β is a repeated zero of f, then the proof of Proposition 1.4 show that β is a zero of f' as well. On the other hand, if β is a single zero of f, then we have

$$f = (x - \beta)g, \qquad \text{with } g \in \overline{K}[x] \text{ such that } g(\beta) \neq 0. \tag{12}$$

In this case we see that $f' = g + (x - \beta)g'$, so that indeed

$$f'(\beta) = g(\beta) + (\beta - \beta)g'(\beta) = g(\beta) \neq 0. \tag{13}$$

♡

Remark 1.7. The criterion in Proposition 1.6 leads to the "right" extension of the notion of separability to the context of rings. Suppose that $\varphi : R \to S$ is a ring homomorphism. Then by applying φ to the coefficients of polynomials in $R[x]$, we can interpret polynomials in $R[x]$ as polynomials in $S[x]$. We can then define

an element $s \in S$ to be ÉTALE over R if there exists some polynomial $f \in R[x]$ such that $f(s) = 0$ in S and moreover f and its derivative f' are comaximal in $R[x]$ in the sense that

$$(f, f') = R[x]. \tag{14}$$

The ring homomorphism φ is itself called étale if every element of S is étale over R. Such homomorphisms are used in algebraic geometry as an appropriate generalization of unramified maps. Intuitively, one can think of them as maps without any critical points, that is, maps with a well-defined non-zero slope everywhere. As one might suspect, an algebraic analog of differentials is useful when formulating this notion; it leads to the definition of so-called DERIVATIONS and KÄHLER DIFFERENTIALS on rings. ❁

2 Separability for fields

As in the last chapter, it turns out to be advantageous to shift the focus from polynomials to (algebraic) field extensions.

Definition 2.1. Let $L|K$ be an algebraic field extension, and let $\beta \in L$. We say that β is SEPARABLE over K if it the zero of a separable polynomial in $K[x]$. Moreover, we say that the extension $L|K$ is separable if every element of L is separable over K. ✌

For a given element, we can test for separability by means of the minimal polynomial.

Proposition 2.2. *Let $L|K$ be an algebraic field extension, and let $\beta \in L$. Then β is separable over K if and only if its minimal polynomial over K is separable.*

Proof. If the minimal polynomial f of β is separable, then the same is the case for β as $f(\beta) = 0$. Conversely, suppose that β is separable over K, so that $g(\beta) = 0$ for some separable polynomial $g \in K[x]$. The minimal polynomial f of β divides g in $M[x]$ for any extension $M|K$, and since g has no repeated zeros for any such extension, the same must be true for its factor f, showing that f is indeed a separable polynomial. ♡

Let us first show that inseparability is never an issue for fields of characteristic 0 and for finite fields.

Proposition 2.3. *Let $L|K$ be an algebraic field extension with L and K of characteristic 0. Then $L|K$ is separable.*

Proof. This is a consequence of Proposition 2.2 and Proposition 1.4. ♡

Proposition 2.4. *Let $L|K$ be a field extension with L and K finite. Then $L|K$ is separable.*

Proof. Let $q = \#L$. The theory of finite fields shows that every element β of L is a zero of the polynomial $f = x^q - x \in K[x]$. Now

$$f' = qx^{q-1} - 1 = -1 \in K[x], \tag{15}$$

Proposition 1.6 therefore implies that f is separable, and therefore the same is true for β. Since β was arbitrary, we have indeed shown that $L|K$ is indeed separable. ♡

Finally, if the characteristic p of the ground field K is finite, then separability is still automatic for finite extensions whose degree is coprime to p.

Proposition 2.5. *Let $L|K$ be a finite extension of fields of characteristic p. If p does not divide $[L:K]$, then $L|K$ is separable.*

Proof. Let $\beta \in L$, and let f be the minimal polynomial of β over K. Then $\deg(f) = [K(\beta):K]$ divides $[L:K]$ by the tower law. Therefore $\deg(f)$ is not divisible by p, so that f, and therefore β itself, is separable by Proposition 1.5. Since β was an arbitrary element of L, the proof is complete. ♡

Proposition 2.3 to 2.5 give a partial answer to Question (ii) in the introduction to this chapter. They show that inseparability is a rather specialized phenomenon. However, it is still relevant, as it is often encountered when studying geometric objects over fields characteristic p; also see Remark 3.11 at the end of this chapter. We therefore consider it in some detail.

Let us start by by formulating a more intrinsic way of understanding the separability of a field extension, namely by relating it to the number of embeddings of such an extension into an algebraic closure of the base field.

Definition 2.6. Let $L|K$ be an algebraic field extension, and let $\overline{K}$ be an algebraic closure. We define $\mathrm{Hom}_K(L,\overline{K})$ to be the set of K-homomorphisms $\varphi : L \to \overline{K}$. ✌

For a generalization of the upcoming theorem, see Exercise 2.

Theorem 2.7. *Let $L|K$ be a finitely generated algebraic extension. Then*

$$\#\,\mathrm{Hom}_K(L,\overline{K}) \leq [L:K] \tag{16}$$

and L is separable if and only if equality in (16) holds.

*Proof**. Let us write $L = K(\beta_1,\dots,\beta_r)$ and consider the chain of field extensions

$$L_0 := K \subset L_1 := K(\beta_1) \subset \dots \subset L_r := K(\beta_1,\dots,\beta_r) = L. \tag{17}$$

For $i = 1,\dots,r$, we define f_i to be the minimal polynomial of β_i over L_{i-1}, which is well-defined because $L|K$ is algebraic. Now suppose that such an i is given, along with a K-homomorphism $\psi : L_{i-1} \to \overline{K}$. Let us define

$$n_i = \deg(f_i) = [L_i : L_{i-1}]. \tag{18}$$

Let $z_i \leq n_i$ be the number of zeros of f_i in $\overline{K}$. As in the introduction to the first chapter, we see that any such zero γ_j gives rise to an L_{i-1}-homomorphism

$$\begin{aligned} \varphi_i : L_i = L_{i-1}(\beta) &\to \overline{K} \\ \beta_i &\mapsto \gamma_j. \end{aligned} \tag{19}$$

By definition, such an L_{i-1}-homomorphism is the same thing as a K-homomorphism $\varphi_i : L_i \to \overline{K}$ that extends the given K-homomorphism $\psi : L_{i-1} \to \overline{K}$.

Conversely, any such L_{i-1}-homomorphism $\varphi : L_i \to \overline{K}$ equals one of the φ_i, since $f(\varphi(\beta)) = 0$ by Proposition 1.5. Therefore there exist n_i extensions of ψ from L_{i-1} to L_i.

Now let us start with the inclusion $\psi : K \to \overline{K}$ and move up the chain (17) by repeating the argument from the previous paragraph r times. Using the tower law, we see that the number of K-homomorphisms $\varphi : L \to K$ equals $z_r \dots z_1$, which is at most

$$n_r \cdots n_1 = [L_r : L_{r-1}] \cdots [L_1 : L_0] = [L_r : L_0] = [L : K], \tag{20}$$

thus showing (16).

If $L|K$ is separable, then the β_i are separable over K, and therefore a fortiori over L_{i-1}, so that the minimal polynomials f_i are separable by Proposition 2.2. In this case $z_i = n_i$ for all i, so that equality holds in (16). If instead $L|K$ is inseparable, then we may add an inseparable element to our set of generators β_i, so that we obtain a proper inequality $z_i < n_i$ for some i; since $z_i \leq n_i$ for all i, one such proper inequality already implies that the total number of K-homomorphisms that we obtain is strictly smaller than $n_r \cdots n_1 = [L : K]$. ♡

Remark 2.8. Theorem 2.7 gives us another way to think of separability: an algebraic field extension $L|K$ is separable if and only if it admits the maximal a priori possible number of K-homomorphisms into an algebraic closure $\overline{K}$. In a sense, every extension allows the maximal number of such K-homomorphisms "when counting with multiplicities", but the separability condition demands that the number simply be maximal without any such facetiousness. It is therefore a fairly natural condition… which is why it is usually satisfied. ❁

We can now return to the yoga behind Remark I.1.14 and Exercise I.7: While Definition 2.1 appropriately generalizes the notion of separability from polynomials to elements to fields by means of the universal quantifier, it is still desirable to have a characterization of separability in terms of a chosen set of generators of an extension $L|K$. The upcoming lemma provides such a characterization; also see Exercise 3.

Lemma 2.9. *Let $L = K(\beta_1, \dots, \beta_r)$ be a finitely generated algebraic field extension of a base field K. Then $L|K$ is separable if and only if all elements $\beta_1, \dots, \beta_r$ are separable over K.*

Proof. This follows by using the set of generators $\beta_1, \dots, \beta_r$ in the proof of Theorem 2.7. ♡

In line with this yoga, we can now transfer separability properties from defining polynomials to fields as a whole. The following results allow us to conclude that if the defining polynomial of a splitting field (or of a stem field) is separable, then the same is true for **all** elements of this extension. This is by no means obvious from the definitions and essentially uses the chain argument from the proof of Theorem 2.7.

Corollary 2.10. *Let $L = K[x]/(f)$ be the stem field of an irreducible polynomial $f \in K[x]$. Then $L|K$ is separable if and only if f is separable.*

Proof. Let $\beta = x + (f)$. Then $L = K(\beta)$, and since $f(\beta) = 0$, the irreducible polynomial f is a non-zero scalar multiple of the minimal polynomial of β over K. Now Lemma 2.9 shows that $L|K$ is separable if and only if β is separable over K, and by Proposition 2.2, this is the case if and only if f is separable. ♡

Corollary 2.11. *Let $L = K[x]/(f)$ be the splitting field of a polynomial $f \in K[x]$. Then $L|K$ is separable if f is separable. If f is irreducible, then the converse statement holds as well.*

Proof. Let $\beta_1, \dots, \beta_r$ be the zeros of f in L. Then $L = K(\beta_1, \dots, \beta_r)$. If f is separable, then the same is true for its zeros β_i by definition, so that $L|K$ is separable by Lemma 2.9.

Now suppose that $L|K$ is separable and that f is irreducible. Then f is a non-zero scalar multiple of the minimal polynomial of its zeros β_i over K. Since the elements β_i of the separable extension $L|K$ are themselves separable over K, Proposition 2.2 shows that f is separable. ♡

Remark 2.12. Note the fine print in Corollary 2.11; and indeed, the splitting field of the inseparable polynomial $x^2 \in K[x]$ over K equals K itself, which is nevertheless a separable extension of K. ❁

Having dealt with the theory, it is time for some examples.

Example 2.13. (i) As in Example 1.3, let F be a field of characteristic p and let $K = F(t)$ be the rational function field over F in the variable t. If we let $L = K(\beta) = K(t^{1/p})$, then $L|K$ is a simple extension of degree p, defined by the polynomial

$$f = x^p - t \in K[x]. \tag{21}$$

As we have seen, the polynomial $\overline{K}$ only has the single zero $\beta = t^{1/p}$ in K. We therefore conclude that β is inseparable, and the same is true for the extension $L|K$.

In fact, the elements of the extension $L|K$ that are separable over K are exactly the elements of K itself, because the tower law implies that we have $[K(\gamma) : K] = [L : K]$ for any element γ of L that does not belong to K itself, so that $K(\gamma) = L$. Since L contains the element $t^{1/p}$, which is inseparable over K, Corollary 2.11 implies that its generator γ over K cannot be separable over K.

Given $\gamma \in L \setminus K$, the previous paragraph shows that $K(\gamma) = L$. Therefore the degree of the minimal polynomial g of γ equals $[K(\gamma) : K] = [L : K] = p$. Proposition 1.5 shows that g is a linear polynomial in x^p, that vanishes in γ, so that it in fact equals

$$g = x^p - \gamma^p = (x - \gamma)^p \in K[x]. \tag{22}$$

For example, the minimal polynomial of $1 + \beta + \beta^2$ over K equals

$$x^p - (1 + \beta + \beta^2) = x^p - 1^p - \beta^p - (\beta^p)^2 = x^p - 1 - t - t^2 \in K[x]. \tag{23}$$

(ii) We adjoin a second variable u to the field K in Part (i) to obtain the rational function field $K = F(t,u)$. We can then consider $\beta = t^{1/p}$ and $\gamma = u^{1/p}$ to construct the extension

$$L = K(\beta,\gamma) = F(t^{1/p}, u^{1/p}) \tag{24}$$

of K. By means of the chain

$$K = F(t,u) \subset F(t^{1/p},u) \subset F(t^{1/p},u^{1/p}) = L \tag{25}$$

we see that $[L:K] = p^2$. Now if $\delta \in L$, then the tower law implies that the degree of its minimal polynomial divides p^2. If moreover $\delta \in L \setminus K$, then this degree cannot equal 1. In this case we have that δ is a zero of the polynomial

$$h = (x-\delta)^p = x^p - \delta^p \in K[x], \tag{26}$$

which is therefore its minimal polynomial. In particular, the simple extension $K(\delta)$ is of degree p over K and therefore cannot equal all of L. For example, the minimal polynomial of $\delta = t^{1/p} + u^{1/p} + 2$ over K equals

$$(x - t^{1/p} - u^{1/p} - 2^p)^p = x^p - t - u - 2 \in K[x]. \tag{27}$$

We conclude that the extension $L|K$ is not simple. Moreover, we see that the elements of L that are separable over K are exactly the elements of K itself.

(iii) Note that Proposition 2.4 implies that there also exist extensions $L|K$ of p-power order p^r in characteristic p that are still separable. For example, one can start with one's favorite finite field $K = \mathbb{F}_q$ and consider the extension

$$K \subset L = \mathbb{F}_{q^{p^r}}. \tag{28}$$

❀

We conclude this section with a final important consequence of Lemma 2.9. To state it, we introduce a further notion.

Definition 2.14. Let $L \mid K$ be a field extension. We define the SEPARABLE CLOSURE L_s of K inside L to be the set of elements of L that are separable over K. The separable closure of K in an algebraic closure $\overline{K}$ is often simply denoted by K^{sep}, and called the SEPARABLE CLOSURE OF K (without further qualification). ✌

We can now show that separable closures, like algebraic closures, are indeed fields.

Corollary 2.15. *Let $L|K$ be a field extension. Then the separable closure L_s of K inside L is a subextension of $L|K$.*

Proof. We have to show that given elements β_1 and β_2 of L_s, with β_2 non-zero, the elements $\beta_1 \pm \beta_2$, $\beta_1\beta_2$, and β_1/β_2 of L again belong to L_s. To this end it suffices to show that the subextension $K(\beta_1,\beta_2)$ of $L|K$ is again separable, but this is a consequence of Lemma 2.9. ♡

3 The structure of inseparable extensions

It turns out that we can combine separability and inseparability to describe general algebraic field extensions in characteristic p. For this, we first define the following complement to the notion of a separable field extension.

Definition 3.1. Let $L\,|\,K$ be a field extension, and let $\beta \in L$. We say that β is PURELY INSEPARABLE over K if we have $\beta^q \in K$ for some power q of the characteristic p. We say that the extension $L|K$ is purely inseparable over K if every element of L is purely inseparable over K.

Moreover, we define the PURELY INSEPARABLE CLOSURE L_i of K inside L to be the set of elements of L that are purely inseparable separable over K. The inseparable closure of K in an algebraic closure of K is often called the PURELY INSEPARABLE CLOSURE OF K (without further qualification). ✌

Example 3.2. (i) The argumentation in Example 2.13 shows that the field extensions considered therein are purely inseparable.

(ii) Let $K = \mathbb{F}_p(t)$, and let $L|K$ be the extension of K given by

$$K \subset L = \mathbb{F}_{p^p}(t^{1/p}). \tag{29}$$

Considering the chain

$$K = \mathbb{F}_p(t) \subset \mathbb{F}_{p^p}(t) \subset \mathbb{F}_{p^p}(t^{1/p}) = L \tag{30}$$

shows that $[L : K] = p^2$. The element $t^{1/p}$ of L is purely inseparable over K, since its p-th power t belongs to K.

By contrast, let $\beta \in \mathbb{F}_{p^p}$ be an element of order $p^p - 1$. Then β cannot be purely inseparable. Indeed, let q be a power of p. Then q is coprime to $p^p - 1$, so that we can write

$$1 = aq + b(p^p - 1) \qquad \text{for some } a, b \in \mathbb{Z}. \tag{31}$$

Now if β^q were an element of K, then we would obtain

$$\beta = \beta^1 = \beta^{aq+p^p+1} = \beta^{aq}\beta^{p^p-1} = (\beta^q)^a \cdot 1 = (\beta^q)^a \in K, \tag{32}$$

which is not the case, since the constant polynomial β is not in the field of constants $\mathbb{F}_p$ of K.

We conclude that the extension $L|K$ is neither separable nor purely inseparable. ❀

The terminology in Definition 3.1 makes it plausible that no element of a purely inseparable extension $L|K$ that is not contained in K itself should be separable. The following proposition shows that this is indeed the case.

Proposition 3.3. *Let $L|K$ be a field extension. Then the purely inseparable closure L_i of K in L is a subextension of $L|K$. Moreover, the elements of L that are both separable and purely inseparable over K are exactly the elements of K.*

Proof. For the first part of the proposition, we have to show that given elements β_1 and β_2 of L_i, with β_2 non-zero, the elements $\beta_1 \pm \beta_2$, $\beta_1\beta_2$, and β_1/β_2 of L again belong to L_i. This follows from the observation that if q_1 (respectively q_2) is such that $\beta_1^{q_1} \in K$ (respectively $\beta_2^{q_2} \in K$), then

$$\begin{aligned}(\beta_1 \pm \beta_2)^{q_1q_2} &= \beta_1^{q_1q_2} + \beta_2^{q_1q_2} = (\beta_1^{q_1})^{q_2} + (\beta_2^{q_2})^{q_1} \in K,\\ (\beta_1\beta_2)^{q_1q_2} &= \beta_1^{q_1q_2}\beta_2^{q_1q_2} = (\beta_1^{q_1})^{q_2}(\beta_2^{q_2})^{q_1} \in K,\\ (\beta_1/\beta_2)^{q_1q_2} &= \beta_1^{q_1q_2}/\beta_2^{q_1q_2} = (\beta_1^{q_1})^{q_2}/(\beta_2^{q_2})^{q_1} \in K.\end{aligned} \tag{33}$$

For the second part of the proof, we first observe that the elements α of K are certainly both separable over K (as they have the separable minimal polynomial $x - a \in K[x]$) and purely inseparable over K (as $\alpha^{p^0} = \alpha^1 = \alpha \in K$). Conversely, suppose that $\beta \in L$ is both separable and purely inseparable over K. Choose q such that $\beta^q = \alpha$ is an element of K. Then β is a zero of the polynomial $f = x^q - \alpha$. Now if $\gamma \in \overline{K}$ is such that $\gamma^q = \alpha$, then $f = (x - \gamma)^q$ in $\overline{K}[x]$ by the binomium modulo p. Since the minimal polynomial of β over K has to divide f in $K[x]$, and therefore in $\overline{K}[x]$ as well, Proposition 2.2 implies that the only way for β to be separable is if $\beta = \gamma$ and $q = 1$, in which case $\beta \in K$. ♡

Example 3.4. Proposition 3.3 gives another proof of Example 3.2(ii). Indeed, Proposition 2.4 implies that β is separable, being an element of the finite field $\mathbb{F}_{p^p}$ inside L. As it does not belong to the base field $\mathbb{F}_p(t)$, it therefore cannot be purely inseparable. ❀

We can now show that every algebraic extension splits into a separable and a purely inseparable part.

Theorem 3.5. *Let $L|K$ be an algebraic field extension, and let L_s be the separable closure of K inside L. Then the following statements hold.*

(i) $L_s|K$ is a separable extension.

(ii) $L|L_s$ is an inseparable extension.

Proof. Part (i) is a consequence of the very definition of the separable closure. As for Part (ii), let $\gamma \in L_s$, and let $f \in K[x]$ be its minimal polynomial over K. Then Proposition 1.5 shows that we can write $f = g(x^q)$ for some power q of p and for some separable irreducible polynomial $g \in K[x]$. As γ is a zero of f, we have $0 = f(\gamma) = g(\gamma^q)$.

We see that γ^q is a zero of the irreducible polynomial $g \in K[x]$, which is therefore its minimal polynomial. The separability of the polynomial g then implies that $\gamma^q \in L_s$. Since γ was arbitrary, we see that $L \,|\, L_s$ is indeed an inseparable extension. ♡

Example 3.6. Let us consider the chain of extensions

$$K = \mathbb{F}_p(t) \subset \mathbb{F}_{p^p}(t) \subset \mathbb{F}_{p^p}(t^{1/p}) = L. \tag{34}$$

We claim that the separable closure L_s of K inside L equals the middle link $\mathbb{F}_{p^p}(t)$ in this chain. Indeed, as we have seen in Example 3.2(ii), the extension $\mathbb{F}_{p^p}(t)|K$

is separable. Since L_s contains this subextension of degree p, and $[L : K] = p^2$, we see that either $[L_s : K] = p$ or $[L_s : K] = p^2$. The latter case is impossible, as the tower law would then imply that $L_s = L$, so that the extension $L|K$ would be separable, which we proved not to be the case in Example 3.2(ii).

We conclude that we are in the former case $[L_s : K] = p$, so that the tower law shows that $L_s = \mathbb{F}_{p^p}(t)$. Note that $L|L_s$ is indeed inseparable by Example 1.3. ❀

Remark 3.7. There is no general equivalent of Theorem 3.5 for an inseparable subextension; see Exercise 13. However, see Exercise 14 as well. ❀

Our final result in this chapter gives an explicit criterion for the separable closure of a field to coincide with its algebraic closure. This will also answer to Question (ii) in the introduction to this chapter.

Theorem 3.8. *Let K be a field of characteristic $p > 0$. Then the following statements are equivalent.*

(i) There is an equality $K^{\mathrm{sep}} = \overline{K}$.

(i') Every algebraic extension of K is separable.

(i") Every finite extension of K is separable.

(ii) Every irreducible polynomial in $K[x]$ is separable.

(iii) The Frobenius homomorphism

$$\begin{aligned} \sigma : K &\to K \\ \alpha &\mapsto \alpha^p \end{aligned} \tag{35}$$

is bijective.

Proof. (i) $\Leftrightarrow$ (i'): As the inclusion $K^{\mathrm{sep}} \subset \overline{K}$ always holds, we have $K^{\mathrm{sep}} = \overline{K}$ if and only if every element of $\overline{K}$ is in fact separable over K. Since every subextension of $\overline{K} \mid K$ is algebraic, and conversely every algebraic extension of K can be embedded into $\overline{K}$, we obtain the desired equivalence.

(i) $\Leftrightarrow$ (i"): Since the algebraic closure $\overline{K}|K$ is the union of its finite subextensions, and conversely every finite extension of K admits a K-homomorphism into $\overline{K}$, we again obtain the desired equivalence.

(i) $\Leftrightarrow$ (ii): Suppose first that $K^{\mathrm{sep}} = \overline{K}$, and let $f \in K[x]$ be irreducible. Let $\beta \in \overline{K}$ be a zero of f. Since f is irreducible, it is the minimal polynomial of β over K. Since $\beta \in K^{\mathrm{sep}}$, we obtain that f is separable by Proposition 2.2.

Now suppose that (ii) holds, and let $\beta \in \overline{K}$. Then the minimal polynomial f of β is separable by hypothesis, so that β is indeed separable itself. Since $\beta \in \overline{K}$ was arbitrary, we indeed obtain the desired equality $K^{\mathrm{sep}} = \overline{K}$.

(i) $\Leftrightarrow$ (iii): If σ is not surjective, then there exists an element $\alpha \in K$ such that the polynomial $f = x^p - \alpha \in K[x]$ does not admit a zero in K. If β is a p-th root of α in $\overline{K}$, then we can write $f = (x-\beta)^p$ in $\overline{K}[x]$ by the binomium modulo p. As the minimal polynomial of β divides f and does not equal $x - \beta$, it is inseparable, which implies that $\beta \in \overline{K} \setminus K^{\mathrm{sep}}$.

Conversely, suppose that σ is surjective, and let $\beta \in \overline{K}$, with minimal polynomial $f \in K[x]$. If β is inseparable, then Proposition 1.5 shows that $f = g(x^p)$ for some polynomial $g \in K[x]$. Since σ is surjective, we can find $\alpha_j \in K$ such that

$$g = \alpha_0^p x^m + \alpha_1^p x^{m-1} + \ldots + \alpha_m^p. \tag{36}$$

But then

$$f = \alpha_0^p x^{mp} + \alpha_1^p x^{(m-1)p} + \ldots + \alpha_m^p = (\alpha_0^p x^m + \alpha_1^p x^{(m-1)} + \ldots + \alpha_m)^p. \tag{37}$$

This contradicts the irreducibility of the minimal polynomial f. We conclude that β is in fact separable. Since $\beta \in \overline{K}$ was arbitrary, we see $K^{\text{sep}} = \overline{K}$. ♡

Definition 3.9. A field K that satisfies the equivalent criteria from Theorem 3.8 is called PERFECT. ✌

Example 3.10. (i) Proposition 1.4 shows that every field of characteristic 0 is perfect.

(ii) Proposition 2.4 shows that every finite field is perfect.

(iii) Example 1.3 shows that if $K = F(t)$ is a univariate rational function field over a field F of characteristic p, then K is not perfect. The same is true for multivariate rational function fields over F. ❀

Remark 3.11. To some extent, the whole point of this chapter has been to provide reassurance that most field extensions are separable. In fact, Theorem 3.8 and Example 3.10 show that most base fields are perfect, and any algebraic extension of such a field is separable.

Still, inseparable extensions have a role to play in mathematics. Geometrically, this shows up when studying the "arithmetic" ramification of covering maps, such as $y^p = x$; such a map turns out to have "tame" ramification at isolated points modulo every prime number, except for p, where it all of a sudden ramifies along a whole curve, essentially because of inseparability phenomena. For more complicated covers, being able to say something about such "vertical" ramification is very important in the study of the degeneration of these maps and the arithmetic phenomena that these give rise to. In fact, multiple PhD theses at the Institute for Algebra and Number Theory at Ulm University have been written on this very topic, with no end in sight for now. ❁

4 Exercises for Chapter II

Exercise 1. Let $f \in K[x]$ be a polynomial. Show that if f is separable as an element of $K[x]$, then it is also separable as an element of $M[x]$ for every finite extension M of K.

Exercise 2. Let $L|K$ be an algebraic field extension. Show that $L|K$ is separable if and only if every finite subextension of $L \,|\, K$ satisfies the criterion from Theorem 2.7.

Exercise 3. Generalize Lemma 2.9 to the case where the chosen generating set of $L|K$ is infinite.

Exercise 4. Let $M|K$ be a subextension of a separable extension $L|K$. Show that $L|M$ and $M|K$ are again separable extensions.

Exercise 5. Let $\varphi : L \to L'$ be a K-homomorphism, and let $\beta \in L$.

(i) Show that β is separable over K if and only if the same is true for $\varphi(\beta)$.

(ii) Suppose that L and L' are two algebraic closures of K. Show that φ induces a K-isomorphism between the corresponding separable closures of K.

Exercise 6. Show that the conditions in Theorem 3.8 are equivalent to the following:

(iii') Some non-trivial power of the Frobenius homomorphism is bijective.

Exercise 7. Let $L|K$ and $M|L$ be separable field extensions. The goal of this exercise is to show that the composed extension $M|K$ is again separable.

(i) Let $\gamma \in M$, and let $f \in L[x]$ be the minimal polynomial of γ over $L[x]$. Show that the subextension L' of $L|K$ that is generated over K by the coefficients of f is finite and separable over K.

(ii) Use the separability of $M|L$ to show that $L'(\gamma)$ is finite and separable over K. (Hint: Count the number of K-homomorphisms of $L'(\gamma)$ into an algebraic closure.)

(iii) Conclude that γ is separable over K and that the composition $M|K$ is separable.

(iv) Use an embedding of M into an algebraic closure $\overline{K}$ of K in combination with Exercise 5 to give an alternative proof of (iii).

Exercise 8. Let $L|K$ be a finite extension, and let L_s be the separable closure of K inside L_s. We define the SEPARABLE DEGREE $[L : K]_s$ of the extension $L|K$ by $[L : K]_s = [L_s : K]$. Use Theorem 3.5 and the prolongation lemma I.1.4 to show that

$$[L : K]_s = \#\mathrm{Hom}_K(L, \overline{K}).$$

Exercise 9. Let $M|L|K$ be a tower of finite extensions. Show that

$$[M : K]_s = [M : L]_s[L : K]_s.$$

Exercise 10. Let F be a perfect field of characteristic p, let t be a variable, and let

$$K = F(t, t^{1/p}, t^{1/p^2}, \ldots).$$

Show that K is a perfect field as well.

Exercise 11. Let $L|K$ and $M|L$ be purely inseparable field extensions. Show that the composition $M|K$ is purely inseparable as well.

Exercise 12. Let $L|K$ be a finite extension. Show that $[L_i : K]$ is a power of the characteristic of K.

Exercise 13. Let $K = \mathbb{F}_2(t)$ be a rational function field over $\mathbb{F}_2$, let f be the irreducible polynomial

$$f = x^6 + x^2 + t \in K[x],$$

and let L be the stem field of f over K.

(i) Let $\alpha = x + (f) \in L$. Show that $L_s = K(\alpha)$.

(ii) Show that $L_i = K$.

(iii) Show that $[L : L_s] \neq [L_i : K]$.

(iv) Show that $[L : K] \neq [L_s : K][L_i : K]$.

(v) Show that $L|L_i$ is inseparable.

Exercise 14. Let $L|K$ be a finite normal extension.

(i) Show that $[L : L_s] = [L_i : K]$.

(ii) Show that $[L : K] = [L_s : K][L_i : K]$.

(iii) Show that $L|L_i$ is separable.

Exercise 15. For each of the following pairs K and f, determine whether the polynomial f is separable over K.

(i) $K = \mathbb{Q}$, $f = x^3 - 2$.

(ii) $K = \mathbb{F}_{17}$, $f = x^3 - 2$.

(iii) $K = \mathbb{F}_3$, $f = x^3 - 2$.

(iv) $K = \mathbb{Q}$, $f = x^5 - 7x^4 + 4x^3 - 28x^2 + 4x - 28$.

(v) $K = \mathbb{Q}$, $f = x^5 - 7x^4 - 3x^3 + 21x^2 - 10x + 70$.

(vi) $K = \mathbb{F}_7$, $f = x^5 - 7x^4 - 3x^3 + 21x^2 - 10x + 70$.

(vii) $K = \mathbb{Q}$, $f = x^7 + x^5 + 3x^4 - 16x^3 - 12x^2 + 20x + 12$.

Exercise 16. Find an irreducible polynomial with coefficients in $\mathbb{Z}$ that is separable, but that is inseparable modulo the prime 1009.

Exercise 17. For devout non-believers: State and prove all the results in this chapter without making use of an algebraic closure.

Summary and main notions of the chapter

With the notions in this chapter, we can phrase the answers to the Questions (i) and (ii) in its introduction as follows:

(i) Proposition 2.2 shows that the irreducible polynomials in $K[x]$ with repeated zeros in $\overline{K}$ are exactly the minimal polynomials of inseparable elements of $\overline{K}$. Moreover, given an irreducible polynomial $f \in K[x]$, we can check whether it is separable by means of Proposition 1.6. If it is not, then the form of f is described more closely by Proposition 1.5.

(ii) Since square-free polynomials over $K[x]$ remain square-free over extensions of K if and only if the same is true for the irreducible polynomials in $K[x]$, this question can be rephrased by asking for which fields K all irreducible polynomials in $K[x]$ are separable. Theorem 3.8 shows that this happens if and only if K is perfect, and Example 3.10 shows that all fields of characteristic zero, as well as finite fields, are perfect. This includes most fields that you will encounter in everyday life, unless you take up the specialized part of arithmetic geometry mentioned in Remark 3.11.

The key skills to take away from this are the following:

– You are able to define the notion of separability for polynomials (Definition 1.1) as well as for fields and their elements (Definition 2.1), and you can indicate the connection between separability and embeddings into the algebraic closure (Theorem 2.7).

– You can formulate simple criteria for a field extension to be separable (Propositions 2.3 to 2.5) and you are able to check whether a given polynomial is separable (Proposition 1.6).

– You are aware of the existence of the separable closure of a given field extension (Corollary 2.15) and can describe the resulting factorization of an arbitrary field extension as the composition of a separable extension with a purely inseparable extension (Theorem 3.5).

Chapter III

Galois extensions

Heretofore we have summarized the notion of a normal field extension by stating that it has a pleasing amount of symmetry; see Remark I.1.7(i). Now the mathematical concept of symmetry is captured by the notion of a group, and indeed, if $L|K$ is a field extension, normal or not, then the set

$$\mathrm{Aut}(L|K) = \{\sigma : L \to L \text{ a } K\text{-automorphism of } L\}, \tag{1}$$

is a group under composition. Because of our motivation of the notion of normality, we would expect normal extensions to have "large" automorphism groups — but it is not quite clear what that should mean concretely.

This means that we should go and explore. Let us see if we can describe automorphism groups of fields, and if we can say how large these groups can get. We start with the simplest possible case, namely that of a simple extension

$$L = K[x]/(f), \tag{2}$$

where $f \in K[x]$ is an irreducible polynomial of degree n say.

Let us denote the canonical element $x + (f)$ of L by β. Since $L = K[x]/(f)$, Noether's isomorphism theorem implies that a K-homomorphism $\sigma : L \to L$ can equally well be described by means of a K-homomorphism

$$\begin{aligned} \varphi : K[x] &\to L \\ x &\mapsto \beta' \end{aligned} \tag{3}$$

that vanishes on the ideal (f). The theory of polynomial rings shows that the ring homomorphism φ in (3) is completely determined by the image β' of the variable x; it can be considered as the evaluation in β'. It remains to see when φ vanishes on the principal ideal (f). Since $\varphi(f) = f(\beta')$, this is the case if and only if $\beta' \in L$ is a zero of f. Conversely, if β' is such a zero, then the K-homomorphism

$$\begin{aligned} \sigma : L &\to L \\ \beta &\mapsto \beta' \end{aligned} \tag{4}$$

that it gives rise to is in fact an automorphism. After all, L is of finite dimension over K, and like any field homomorphism, σ is injective, so that it is an isomorphism by the rank-nullity theorem.

We conclude that the underlying set of the group $\mathrm{Aut}(L|K)$ is in bijection with the set of zeros β' of f in $L = K[x]/(f)$. This description is already quite explicit; in particular, it shows that determining the cardinalityof $\mathrm{Aut}(L|K)$ comes down to determining the number of zeros of f in $K[x]/(f)$. Now since the polynomial f is of degree n, division with remainder implies that it admits at most n zeros in the field L. We see that $\mathrm{Aut}(L|K)$ contains at most n elements. Moreover, for actual equality $\#\mathrm{Aut}(L|K)$ to hold, we need that f admits exactly n zeros over L. For this to happen, we need that f splits into linear factors over $L = K[x]/(f)$; but Corollary I.1.13 shows that this is the case if and only if L is **normal** over K.

Is this quite enough? No, there is one final subtlety. Even if f does split into linear factors over $L = K[x]/(f)$, we need the zeros of f to be distinct in order to be able to conclude that indeed $\#\mathrm{Aut}(L|K) = n$. In other words, we need that f is a separable polynomial, or equivalently by Corollary II.2.10 that the field extension $L|K$ is **separable**.

All in all, we see that the largest possible cardinality of the automorphism group of the simple extension L of K

$$\#\mathrm{Aut}(L|K) = n = [L : K], \tag{5}$$

and that this equality is attained if and only if $L|K$ is normal and separable.

This is a wonderful result, but we did assume that $L = K[x]/(f)$ was a simple extension throughout. We need to generalize beyond this case. Moreover, while we have obtained results on the cardinality of $\mathrm{Aut}(L|K)$, we have not obtained any useful way to describe its actual group structure. We are therefore led to the following motivating questions for this chapter:

(i) How can we characterize finite extensions $L|K$ whose automorphism group is as "large as possible" beyond the case of simple extensions considered in this introduction?

(ii) How can we determine the structure of $\mathrm{Aut}(L|K)$ as an abstract group?

We can give some sneak peeks into the answer to these questions. As for Question (i), we shall show in generality that the largest possible cardinality of a finitely generated algebraic extension $L|K$ equals the degree $[L : K]$, and once again this cardinality is attained exactly if $L|K$ is normal and separable. Field extensions of this kind are called (finite) Galois extensions, and this chapter will give several criteria that can be used to check whether a given finite extension $L|K$ is a Galois extension.

In an ironic twist, though we will have to put in some work to move beyond the case of simple field extension, our theory can later be used to prove that any finite Galois extension is in fact a simple extension, so that in a sense this generalization is superfluous. However, the ideas behind this generalization are enlightening, and by not relying on any particular generator, our methods become more flexible. This is particular useful when generalizing to the case of infinite Galois extensions, for which no single generator suffices.

Question (ii) is answered by methods similar to those in this introduction. Given an extension $L|K$ as well as an element $\beta \in L$, any K-automorphism

$\sigma : L \to L$ has to map β to another zero of its minimal polynomial f by Proposition I.1.5. In this way, we can study the group $\mathrm{Aut}(L|K)$ by its induced action on the zeros of f. If L is the splitting field of f, then this action is even faithful, so we can study $\mathrm{Aut}(L|K)$ by means of the permutations of the roots of f that it induces; the group $\mathrm{Aut}(L|K)$ can then be interpreted as those permutations of the zeros of f that are "compatible" with the algebraic structure of the extension $L|K$. And this is indeed how Galois visualized his eponymous groups.

But enough sneak peeks; it is time to get started.

1 Bottom-up: Normal and separable

In light of our results for simple extensions, the following makes sense.

Definition 1.1. A field extension $L|K$ is called Galois if it is both normal and separable. ✌

The first theorem in this chapter generalizes the characterization of Galois extensions beyond the simple case considered in its introduction.

Theorem 1.2. *Let $L|K$ be a finite extension of fields, and let*

$$\mathrm{Aut}(L|K) = \{\sigma : L \to L \,:\, \sigma \text{ is a } K\text{-automorphism of } L\}. \tag{6}$$

be its K-automorphism group. Then we have

$$\#\,\mathrm{Aut}(L|K) \leq [L : K], \tag{7}$$

and $L|K$ is Galois if and only equality holds in (7).

Proof. The proof of the (7) can be reduced to an application of Theorem II.2.7. Indeed, the prolongation lemma 1.4 allows us to choose a K-homomorphism $\iota : L \to \overline{K}$. Then by composition with ι, any element $\sigma : L \to L$ of $\mathrm{Aut}(L|K)$ can be interpreted as a K-homomorphism $\varphi = \iota\sigma : L \to \overline{K}$, so that Theorem II.2.7 implies the inequality (7).

The same argument shows that for equality to hold in (7), it is necessary that $L|K$ be separable. Let us therefore assume that this is the case, and let us use the K-isomorphism ι identify L with $\iota(L)$. For (7) to be an equality, we then need that all $[L : K]$ embeddings $\varphi : L \to \overline{K}$ maps L to $\iota(L)$. By Theorem I.1.10 and Remark I.1.12(i), this happens if and only if $L|K$ is normal, so that the theorem is proved. ♡

Remark 1.3. (i) The idea behind Theorem 1.2 is that every K-automorphism $\sigma : L \to L$ can be interpreted as an embedding of L into $\overline{K}$; the separability condition then ensures that there are enough such embeddings, whereas the normality condition ensures that these embeddings all indeed map L to itself (instead of mapping L to some subextension of $\overline{K}$ that instead of being equal to L is merely K-isomorphic to L).

(ii) Those agnostic or actively hostile regarding the existence of the algebraic closure $\overline{K}$ can replace the K-homomorphism $\iota : L \to \overline{K}$ in the proof of Theorem 1.2 by a K-homomorphism $L \to M$, where M is any sufficiently large splitting field that contains L; also see the proof of Theorem I.1.10. ❁

Since we studied normality and separability fairly well, we have quite a few criteria at our disposal to check whether a given finite extension is Galois. The first of these results was considered in the introduction to this chapter. Also see Exercise 2.

Proposition 1.4. *Let $L = K[x]/(f)$ be the stem field of an irreducible polynomial $f \in K[x]$. Then $L|K$ is Galois if and only if the following two conditions hold.*

(i) f splits into linear factors over L.

(ii) f is separable.

Proof. This follows from Definition 1.1 since Condition (i) is equivalent to the normality of $L|K$ by Corollary I.1.13 and Condition (ii) is equivalent to the separability of $L|K$ by Corollary II.2.10. ♡

Proposition 1.5. *Let L be the splitting field of an irreducible polynomial $f \in K[x]$. Then $L|K$ is Galois if f is separable. If f is irreducible, then the converse statement holds as well.*

Proof. Since $L|K$ is normal by Theorem 1.6, the extension $L|K$ is Galois if and only if it is separable, so that the result is a consequence of Corollary II.2.11. ♡

Corollary 1.6. *Let $L|K$ be a field extension with L and K finite. Then $L|K$ is Galois.*

Proof. This follows from Corollary I.1.8 and Proposition II.2.4. ♡

It is time to look at a broad range of examples.

Example 1.7. (i) Let $L|K$ be a quadratic field extension (meaning that $[L : K] = 2$). If $\beta \notin K$, then $K(\beta) \neq K$. Applying the tower law to the chain

$$K \subsetneq K(\beta) \subset L, \tag{8}$$

we obtain

$$[L : K(\beta)][K(\beta) : K] = [L : K] = 2. \tag{9}$$

Since $[K(\beta) : K] > 1$, this can only happen if $[L : K(\beta)] = 1$, so that $L = K(\beta)$ and $[K(\beta) : K] = [L : K] = 2$. We conclude that the minimal polynomial f of β is of the form

$$f = x^2 + \alpha_1 x + \alpha_0 \in K[x]. \tag{10}$$

Example I.1.3(i) shows that $[L : K]$ is normal, so that Proposition 1.4 implies that $L|K$ is Galois if and only if f is **separable**. Proposition II.2.5 shows that this is automatic as long as $\mathrm{char}(K) \neq 2$; in this case $L|K$ is both the stem field and the splitting field of f, and by completing the square we can also write

$$L = K(\sqrt{\alpha_1^2 - 4\alpha_0}). \tag{11}$$

An example of a Galois extension of this kind is given by the stem field of

$$f = x^2 - 2 \in \mathbb{Q}[x]. \tag{12}$$

On the other hand, if $\mathrm{char}(K) \neq 2$, then the polynomial (10) may be **inseparable**. In fact, if f is of the form $x^2 - \alpha$, then over L we have

$$f = (x-\beta)(x+\beta) = (x-\beta)^2 \in L[x], \tag{13}$$

with $\beta \in L$ such that $\beta^2 = \alpha$. We see that the minimal polynomial f of β, and with it the quadratic extension $L|K$, is inseparable. An example is provided by the stem field of

$$f = x^2 - t \in K[x] \tag{14}$$

over $K = \mathbb{F}_2(t)$; see Example 1.3.

Instead, in characteristic 2 quadratic polynomials with non-trivial linear term are indispensable in order to construct quadratic Galois extensions of K. For example, for $K = \mathbb{F}_2$ the polynomial

$$f = x^2 + x + 1 \in \mathbb{F}_2[x] \tag{15}$$

is irreducible, as it is of degree $2 \leq 3$ and does not have a zero in its ground field $\mathbb{F}_2$. It therefore defines the extension $L = \mathbb{F}_4$, which is Galois over $K = \mathbb{F}_2$ by Corollary 1.6. And indeed, if $\beta \in \mathbb{F}_4$ is a zero of f, then ignoring signs, as we may in fields of characteristic 2, we obtain

$$(x+\beta)(x+\beta+1) = x^2 + (2\beta+1)x + (\beta^2+\beta) = x^2 + x + 1 = f \in L[x], \tag{16}$$

thus showing that f is indeed separable, as is also implied by Proposition 1.4 considering the fact that $L|K$ is Galois.

(ii) Suppose that $L|K$ is a cubic field extension. As in Part (i), we see that $L = K(\beta)$ for any element $\beta \in L \setminus K$. Let $f \in K[x]$ be the minimal polynomial of β over K. Then $\deg(f) = 3$. Suppose first that f is **separable**. Then we can factor f in $L[x]$, and there are two possibilities:

(a1) $f = (x-\beta)q$ with q quadratic and irreducible: In this case the introduction to this chapter shows that $\mathrm{Aut}(L|K) = 1$. In particular, $L|K$ is not a Galois extension.

The splitting field of f is still Galois by Proposition 1.5, but it is of degree 6 over K, as we need to adjoin a zero of the quadratic polynomial q to L to obtain it. An example of this behavior is provided by the polynomial

$$f = x^3 - 2 \in \mathbb{Q}[x], \tag{17}$$

which splits into a linear and a quadratic factor over the stem field $L = \mathbb{Q}(\sqrt[3]{2})$ by Example 1.3(ii).

(a2) $f = (x-\beta)(x-\beta')(x-\beta'')$ for β, β', β'' distinct: In this case Proposition 1.4 shows that $L|K$ is Galois. Its Galois group is of cardinality $\#\mathrm{Gal}(L|K) = [L:K] = 3$. Since 3 is a prime number, we conclude that $\mathrm{Gal}(L|K)$ is cyclic, and generated by any of its non-trivial elements.

An example of this behavior occurs for the polynomial

$$f = x^3 - x^2 - 2x + 1 \in \mathbb{Q}[x] \tag{18}$$

from Example III.1.9(ii). Alternatively, we can consider the polynomial

$$f = x^3 - 2 \in K[x] \tag{19}$$

over $K = \mathbb{Q}(\zeta_3)$ instead. Over this field, it splits as

$$f = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}) \in L[x]. \tag{20}$$

Note that f is indeed irreducible over K, as it is cubic and does not admit a zero in K. After all, if it did, then the cubic stem field of f over $\mathbb{Q}$ could be realized as a subfield of the quadratic number field $\mathbb{Q}(\zeta_3)$, which is impossible by the tower law.

If f is **inseparable** instead, then we either have $f = gh^2$ or $f = h^3$ for distinct linear polynomials $g, h \in \overline{K}[x]$. The former case cannot occur; in this case we would obtain that $f' = h(2gh' + g'h) = h(2g + h)$, so since $2g + h$ has no zeros in common with g and h, the greatest common divisor of f and f' would equal h. As this greatest common divisor can already be computed over $K[x]$, we obtain a contradiction with the irreducibility of f over K. We are therefore left with a final possibility:

(b1) $f = (x - \beta)^3$: In this case the introduction to this chapter shows that $\mathrm{Aut}(L\,|\,K)$ is trivial, even though $L\,|\,K$ is not a trivial extension. In particular, $L\,|\,K$ is not a Galois extension, though it is normal, being the splitting field of f is L itself. Note that this case can occur only in characteristic 3 by Proposition II.1.5. An example of this behavior is provided by the polynomial

$$f = x^3 - t \in K[x] \tag{21}$$

over the field $K = \mathbb{F}_3(t)$; see Example 1.3.

(iii) We apply Proposition 1.4 to the polynomial

$$f = x^4 - 2 \in \mathbb{Q}[x], \tag{22}$$

which is irreducible by the Eisenstein criterion. Since separability is automatic over $\mathbb{Q}$ by Proposition II.1.4, it remains to see whether f splits into distinct linear factors over a field $L \subset \mathbb{C}$ that is obtained by adjoining one of its zeros. Taking $\beta = \sqrt[4]{2}$, we obtain

$$L = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \subset \mathbb{C}. \tag{23}$$

Though f has two zeros in L, namely $\pm\beta$, it does not in fact split into linear factors over L, as its other two imaginary zeros $\pm\beta i$ are not contained in $\mathbb{R}$, and therefore not in L either. We conclude that the stem field L of f is not Galois. In fact the various embeddings of L into $\mathbb{C}$ have two possible images, namely

$$\mathbb{Q} \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\beta^2 \oplus \mathbb{Q}\beta^3 \quad \text{and} \quad \mathbb{Q} \oplus \mathbb{Q}\beta i \oplus \mathbb{Q}\beta^2 \oplus \mathbb{Q}\beta^3 i, \tag{24}$$

which is in line with Theorem I.1.10 since L is not normal over $\mathbb{Q}$.

By contrast, the splitting field of the polynomial $f = x^4 - 2 \in \mathbb{Q}[x]$ is still Galois by Proposition 1.5 and Proposition II.1.4. In Example 4.4(iii) we shall determine the automorphism group of this splitting field over $\mathbb{Q}$. ❀

Automorphism groups of Galois extensions have a special name.

Definition 1.8. Let $L|K$ be a Galois extension. Then we define the GALOIS GROUP $\mathrm{Gal}(L|K)$ by

$$\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K). \tag{25}$$

✌

2 Top-down: Fixed fields

Galois extensions are essentially the most well-behaved field extensions in existence. The criteria so far have mostly considered when an extension of a given base field is finite, but it turns out to be equally useful to know which subfields K of a given field L have te property that $L|K$ is Galois. To give the most useful criterion of this kind, we need an important notion that will also play a crucial role in the next chapter.

Definition 2.1. Let $L|K$ be a field extension, and let $G \subset \mathrm{Aut}(L|K)$ be a subgroup. We define the FIXED FIELD L^G of G as the subextension

$$L^G = \{\beta \in L \,:\, \sigma(\beta) = \beta \text{ for all } \beta \in G\} \tag{26}$$

of $L|K$. ✌

Remark 2.2. Exercise 4 shows that L^G is indeed a field. One this is known, it follows that $L^G \,|\, K$ is a well-defined field extension, because certainly all elements of K are fixed under the elements of a subgroup of $\mathrm{Aut}(L|K)$; indeed, since the elements of $\mathrm{Aut}(L|K)$ are K-automorphisms, they fix all the elements of K by definition, so that $K \subset L^G$. ❁

Using fixed fields allows us to state the following theorem on the interaction between groups and fixed fields, which we shall exploit in the main theorem of Galois theory in the next chapter.

Theorem 2.3. *Let $L|K$ be a field extension.*

(i) If $G \subset \mathrm{Aut}(L|K)$ is a finite subgroup, then $L|L^G$ is a finite Galois extension with $\mathrm{Gal}(L|L^G) = G$.

(ii) If $L|K$ is a finite Galois extension, then $G = \mathrm{Aut}(L|K)$ is a finite group with $L^G = K$.

Proof.* (i): Let us denote $M = L^G$. We start the proof by showing that the extension $L|M$ is normal and separable (though this is strictly speaking superfluous; see Exercise 6). To this end, let $\beta \in L$, and let $f \in M[x]$ be its minimal polynomial over M. Suppose that $\sigma \in G$. Since σ fixes $M = L^G$ by the very definition of the

latter field, Proposition 1.5 shows that $\sigma(\beta)$ is again a zero of f for all $\sigma \in G$. Now let

$$Z = \{\sigma(\beta) \,:\, \sigma \in G\} \subset L \tag{27}$$

be the finite set of elements of L thus obtained by varying $\sigma \in G$. Then we can form the polynomial

$$g = \prod_{\gamma \in Z} (x - \gamma) \in L[x]. \tag{28}$$

Then in fact g equals the minimal polynomial f of β over M. Indeed, since we have shown that all $\gamma \in Z$ are again zeros of f, and these elements are all simple zeros of g by construction, we have $g \mid f$ in $L[x]$. Moreover, since any element $\sigma \in G$ is a bijection, applying it to the elements of the G-orbit Z permutes the elements of this orbit. This implies that $\sigma(g) = g$ for all $\sigma \in G$, so that all coefficients of g are fixed by σ and therefore $g \in M[x]$ by definition of $M = L^G$. The resulting division relation $g \mid f$ in $M[x]$ along with the irreducibility of $f \in M[x]$ then implies that indeed $g = f$, Thus we have reconstructed the minimal polynomial over $M[x]$ of any given element β of L.

To show that $L|K$ is normal, suppose that $f \in M[x]$ is an irreducible polynomial with a zero β in L. We just showed that f is the polynomial g from (28); in particular, f splits into linear factors over L. This proves normality of $L|M$ since $f \in M[x]$ was arbitrary. Since g has single zeros, we also see that $\beta \in L$ is separable over M, and since $\beta \in L$ was arbitrary, we also see that the field extension $L|M$ is separable. It is therefore indeed Galois.

Let $n = \#G$. It remains to show that the extension $L|M$ is of degree n. We first show that $[L : M] \leq n$. To this end, it suffices to show that if we have any set of $m > n$ elements $\beta_1, \ldots, \beta_m$ in L, then these elements are linearly dependent over M. Let us enumerate the elements $\sigma_1, \ldots, \sigma_n$ of G. Linear algebra shows that the homogeneous linear system of n equations

$$\left\{ \begin{array}{rcl} \sigma_1(\beta_1)x_1 + \ldots + \sigma_1(\beta_m)x_m & = & 0, \\ \vdots & \vdots & \\ \sigma_n(\beta_m)x_1 + \ldots + \sigma_n(\beta_m)x_m & = & 0, \end{array} \right. \tag{29}$$

in the $m > n$ variables $x_1, \ldots, x_m$ has a non-zero solution $(\gamma_1, \ldots, \gamma_m)$ in L^m. We will show that it even has a non-zero solution in M^m.

To this end, let us choose a non-zero solution $(\gamma_1, \ldots, \gamma_m) \in L^m$ of (29) in such a way that its number of non-zero entries is minimal among the set of all non-zero solutions of (29) in L^m. Renumbering the β_j if necessary, we may assume that $\gamma_1 \neq 0$, so that $\gamma_1 \in M$ after a suitable rescaling. We then claim that in fact

$$(\gamma_1, \ldots, \gamma_m) \in M^m. \tag{30}$$

Indeed, let $\sigma \in G$. Applying σ to the system of equations

$$\left\{ \begin{array}{rcl} \sigma_1(\beta_1)\gamma_1 + \ldots + \sigma_1(\beta_m)\gamma_m & = & 0, \\ \vdots & \vdots & \\ \sigma_n(\beta_m)\gamma_1 + \ldots + \sigma_n(\beta_m)\gamma_m & = & 0, \end{array} \right. \tag{31}$$

and using that σ, being a field homomorphism, is compatible with addition and multiplication, we obtain

$$\begin{cases} (\sigma\sigma_1)(\beta_1)\sigma(\gamma_1)+\ldots+(\sigma\sigma_1)(\beta_m)\sigma(\gamma_m) &= 0, \\ \vdots & \vdots \\ (\sigma\sigma_n)(\beta_1)\sigma(\gamma_1)+\ldots+(\sigma\sigma_n)(\beta_m)\sigma(\gamma_m) &= 0. \end{cases} \tag{32}$$

Now since the automorphisms $\sigma_1,\ldots,\sigma_n$ constitute a group (namely G), it is stable under left multiplication by σ. Therefore the system (32) can be rearranged to

$$\begin{cases} \sigma_1(\beta_1)\sigma(\gamma_1)+\ldots+\sigma_1(\beta_m)\sigma(\gamma_m) &= 0, \\ \vdots & \vdots \\ \sigma_n(\beta_1)\sigma(\gamma_1)+\ldots+\sigma_n(\beta_m)\sigma(\gamma_m) &= 0. \end{cases} \tag{33}$$

This implies that $(\sigma(\gamma_1),\ldots,\sigma(\gamma_m))$ is a solution in L^m to the system (29), just as the original tuple $(\gamma_1,\ldots,\gamma_m)\in L^m$ was. The same is therefore true for their difference

$$(\sigma(\gamma_1)-\gamma_1,\ldots,\sigma(\gamma_m)-\gamma_m)\in L^m. \tag{34}$$

Since $\sigma(\gamma_j)=0$ if $\gamma_j=0$, the new solution (34) has zero entries wherever this was the case for the original solution $(\gamma_1,\ldots,\gamma_m)\in L^m$. Moreover, since γ_1 was assumed to be non-zero, and $\sigma(\gamma_1)=\gamma_1$ since $\gamma\in M$, we see that the new solution (34) has at least one more zero entry than the original solution. By minimality of the latter solution, this implies that the new tuple (34) is identically zero. Since σ was arbitrary, this shows that $\sigma(\gamma_j)=\gamma_j$ for all $\sigma\in G$ and for all $1\le j\le m$. This means that $\gamma_j\in M=L^G$ for all $1\le j\le m$, which shows that indeed $(\gamma_1,\ldots,\gamma_m)\in M^m$, as claimed in (30).

Now since one of the automorphisms σ_i equals the identity homomorphism, inspection of the corresponding i-th row of (31) yields

$$0=\sigma_i(\beta_1)\gamma_1+\ldots+\sigma_i(\beta_m)\gamma_m=\beta_1\gamma_1+\ldots+\beta_m\gamma_m \tag{35}$$

We have obtained the desired linear dependence, and we conclude that indeed

$$\#G=:n\ge[L:M]. \tag{36}$$

We have already shown that $L|M$ is a Galois extension, so that $\#\mathrm{Aut}(L|M)=[L:M]$ as well by Theorem 1.2. Since have $G\subset\mathrm{Aut}(L|M)$ by construction of $M=L^G$, Equation (36) implies the equality $G=\mathrm{Aut}(L|M)$.

(ii): Let $n=[L:K]$. Then $n=\#G$ by Theorem 1.2, and from Part (i) we obtain that $L|L^G$ is another extension with $[L:L^G]=n$. Applying the tower law, we obtain

$$n=[L:K]=[L:L^G][L^G:K]=n[L^G:K], \tag{37}$$

so that $[L^G:K]=1$ and therefore $K=L^G$. ♡

Remark 2.4. The crux of the argument in the proof of Theorem 2.3 is the proof that $[L:L^G]=\#G$. The subtle linear-algebraic argument is due to Emil Artin, who used it in his seminal work [Art98]. Note that the underlying idea, that the automorphism group of $L|L^G$ is G itself (and no larger) is quite plausible a priori and certainly memorable a posteriori. ❁

Our proof of Theorem 2.3 yields the following useful corollary.

Corollary 2.5. *Let $L|K$ be a finite Galois extension, and let $\beta \in L$. If*

$$Z = \{\sigma(\beta) \,:\, \sigma \in \mathrm{Gal}(L|K)\} \tag{38}$$

is the orbit of β under the action of $\mathrm{Gal}(L|K)$, then the minimal polynomial f of β over K is given by

$$f = \prod_{\gamma \in Z} (x - \gamma) \in K[x]. \tag{39}$$

Remark 2.6. There is an alternative proof of Theorem 2.3 that avoids the use of the techniques in Corollary 2.5; see Exercise 6. ❁

We can now also show that every finite Galois extension arises by taking appropriate fixed fields.

Corollary 2.7. *Let $L|K$ be a finite extension. Then $L|K$ is Galois if and only if $K = L^G$ for some subgroup $G \subset \mathrm{Aut}(L|K)$, in which case $\mathrm{Gal}(L|K) = G$.*

Proof. If $L|K$ is Galois, then Theorem 2.3(ii) shows that $L = K^G$ for $G = \mathrm{Aut}(L|K)$. Conversely, if $K = L^G$ for some $G \subset \mathrm{Aut}(L|K)$, then $L|K$ is Galois, so that $\mathrm{Aut}(L|K) = G$ by Theorem 2.3(i). ♡

Example 2.8. Let $L|K$ be an extension of finite fields, with $\#K = q$ say. Then $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$ for some $n \geq 1$. Corollary 1.6 shows that $L|K$ is Galois, but we can also use Theorem 2.3 to see this. Indeed, the theory of finite fields shows that K is the fixed field of the q-Frobenius automorphism

$$\begin{aligned} \sigma_q : L &\to L \\ \beta &\to \beta^q. \end{aligned} \tag{40}$$

If we therefore let $G = \langle \sigma \rangle \subset \mathrm{Aut}(L|K)$, then Corollary 2.7 implies that $G = \mathrm{Gal}(L|K)$. In particular, we obtain that $\#G = n$.

We conclude that we have $\mathrm{ord}(\sigma_q) = n$ for $\sigma_q \in \mathrm{Aut}(L|K)$. Another way to see this is using the theory of finite fields yet again to observe that while all elements of L are fixed under $\sigma_q^n = \sigma_{q^n}$, they are not fixed under any smaller non-trivial power of σ_q. ❀

3 Example: Symmetric polynomials

Theorem 2.3 is also related to the theory of symmetric polynomials, whose main results we consider in this section.

Proposition 3.1. *Let k be a field, and let $R = k[x_1, \ldots, x_n]$ be a polynomial ring in $n > 0$ variables over k. Given $\sigma \in S_n$, there exists a unique automorphism*

$$\begin{aligned} \alpha_\sigma : R &\to R \\ x_i &\mapsto x_{\sigma(i)} \end{aligned} \tag{41}$$

that restricts to the identity on k, and the map $\sigma \mapsto \alpha_\sigma$ defines an action of S_n on R.

Proof. The fact that σ is well-defined and unique is a consequence of the universal property of polynomial rings. To see that we indeed obtain an action, let $\sigma, \tau \in S_n$. Then for all k between 1 and n we have

$$\alpha_{\sigma\tau}(x_k) = x_{(\sigma\tau)(k)} = x_{\sigma(\tau(k))} = \alpha_\sigma(x_{\tau(k)}) = \alpha_\sigma(\alpha_\tau(x_k)) = (\alpha_\sigma\alpha_\tau)(x_k). \tag{42}$$

The uniqueness in the first part of the proposition then implies that

$$\alpha_{\sigma\tau} = \alpha_\sigma\alpha_\tau, \tag{43}$$

which was to be shown. ♡

Definition 3.2. Let k be a field, and let an integer $n > 0$ be given. Then we define the (ELEMENTARY) SYMMETRIC POLYNOMIALS $s_1, \ldots, s_n$ by means of the equalities

$$\begin{aligned} s_1 &= \sum_{1 \le i_1 \le n} x_i = x_1 + \ldots + x_n, \\ s_2 &= \sum_{1 \le i_1 < i_2 \le n} x_i x_j, \\ &\vdots \\ s_n &= \sum_{1 \le i_1 < \ldots < i_n \le n} x_{i_1} \cdots x_{i_j} = x_1 \cdots x_n. \end{aligned} \tag{44}$$

✌

Theorem 3.3. *Let k be a field, and let $R = k[x_1, \ldots, x_n]$ be a polynomial ring in $n > 0$ variables over k.*

(i) The elementary symmetric polynomials are symmetric, in the sense that given i between 1 and n we have $\alpha_\sigma(s_i) = s_i$ for all $\sigma \in S_n$.

(ii) Conversely, suppose that $f \in k[x_1, \ldots, x_n]$ is symmetric. Then there exists a unique polynomial $g \in k[y_1, \ldots, y_n]$ such that

$$f = g(s_1, \ldots, s_n). \tag{45}$$

*Proof**. (i): As any variable occurs at most once in a given monomial defining the sum s_i, we can describe any such monomial by the set of variables that occurs in it, which always has cardinality i. Moreover, since any such set can be ordered under $<$ in a unique way, we obtain that the set of monomials occuring in s_i is in natural bijective correspondence with the set of subsets of $\{1, \ldots, n\}$ of cardinality i. Since all these monomials occur with identical coefficient, namely 1, and any $\sigma \in S_n$ permutes the subsets of $\{1, \ldots, n\}$ of cardinality i, we obtain that s_i is indeed invariant under the action of S_n on R.

(ii): Let a symmetric polynomial $f \in k[x_1, \ldots, x_n]$ be given, and let us order the terms of f by the graded lexicographic order. In other words, we agree that $\alpha\mathbf{x}^\mathbf{i} \ge \alpha'\mathbf{x}^{\mathbf{i}'}$ for non-zero α and α' if either

$$\sum_{k=1}^{n} i_k > \sum_{k=1}^{n} i'_k \tag{46}$$

or if equality holds in (46) and $\mathbf{i} \geq \mathbf{i}'$ lexicographically, meaning that either $\mathbf{i} = \mathbf{i}'$ or $i_k > i'_k$ for the first index k between 1 and n for which $i_k \neq i'_k$.

We start by showing the existence of a polynomial $g \in k[y_1,\dots,y_n]$ as in (ii). If $f = 0$, then we are done. Otherwise we proceed inductively. Let $\alpha\mathbf{x}^{\mathbf{i}}$ be the first non-zero monomial in f with respect to the graded lexicographic order. Since f is symmetric, and the action of S_n maps monomials to monomials, we see that f also contains $\alpha\mathbf{x}^{\sigma(\mathbf{i})}$ for all $\sigma \in S_n$. This implies that $i_1 \geq \dots \geq i_n$; otherwise some $\alpha\mathbf{x}^{\sigma(\mathbf{i})}$ would be strictly larger with respect to the graded lexicographic order than the monomial $\alpha\mathbf{x}^{\sigma(\mathbf{i})}$ under consideration, in contradiction with our hypothesis.

Since $i_1 \geq \dots \geq i_n$, we can write $\alpha\mathbf{x}^{\mathbf{i}}$ as a product of its constant term with monomials of the form $x_{i_1}\cdots x_{i_r}$ such that $i_1 > \dots > i_r$, say m of them indexed by $j = 1,\dots,m$. Let us define $g = \alpha\prod_{j=1}^{m} y_{r_j}$ accordingly. Then the largest term in $g(s_1,\dots,s_n)$ with respect to the graded lexicographic order is

$$\alpha\prod_{j=1}^{m} x_{i_1}\cdots x_{i_r} \tag{47}$$

which is the same as the larger term of f with respect to the graded lexicographic order by construction.

Now by construction the leading coefficient of $f - g(s_1,\dots,s_n)$ is strictly smaller with respect to the lexicographical ordering than that of f. We see that if we repeat the step above and keep adding suitable new terms $\alpha\prod_{j=1}^{m} y_{r_j}$ to g accordingly, the difference $f - g(s_1,\dots,s_n)$ will eventually be of degree 0 in the variable x_1. Repeating this for the other x_i, we eventually end up with the zero polynomial, as desired.

To show the uniqueness of g, it suffices that we have $g(s_1,\dots,s_n) = 0$ if and only if $g = 0$. To achieve this, it is in turn sufficient to show that distinct monomials in $k[y_1,\dots,y_n]$ give rise to distinct sets of monomials in $k[x_1,\dots,x_n]$ upon substituting $(s_1,\dots,s_n)$, so that no mutual cancellation can occur. For this, let us consider such a monomial $\alpha\mathbf{y}^{\mathbf{j}}$. Then the largest term in $g(s_1,\dots,s_n)$ with respect to the graded reverse lexicographic order is given by

$$\alpha\sum_{i=1}^{n} x_1^{j_1+\dots+j_n} x_2^{j_2+\dots+j_n}\cdots x_n^{j_n}. \tag{48}$$

Since we can recover $(j_1,\dots,j_n)$ from the exponents in (48) by taking additive differences, we obtain the required distinctness of the $\alpha\mathbf{y}^{\mathbf{j}}$, thus concluding the proof of Theorem 3.3. ♡

Rather than understanding the full details of the proof of Theorem 3.3, it is important to understand the illustration of the underlying techniques given by the following examples.

Example 3.4. (i) The symmetric polynomial in 4 variables given by

$$-(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4), \tag{49}$$

is equal to $-s_2$.

(ii) We now consider the symmetric polynomial in 4 variables given by

$$\begin{aligned} &x_1^2x_2x_3 + x_1^2x_2x_4 + x_1^2x_3x_4 + x_1x_2^2x_3 + x_1x_2^2x_4 + x_1x_2x_3^2 \\ &\quad + x_1x_2x_4^2 + x_1x_3^2x_4 + x_1x_3x_4^2 + x_2^2x_3x_4 + x_2x_3^2x_4 + x_2x_3x_4^2. \end{aligned} \tag{50}$$

The first monomial in this expression is the product of x_1 with $x_1x_2x_3$, which are the leading terms of s_1 and s_3. Subtracting the resulting substitution s_1s_3 from (50), we are left with $-4x_1x_2x_3x_4$, which equals $-4s_4$. Therefore we see that (50) is nothing but $s_1s_3 - 4s_4$.

(iii) Finally, we consider the symmetric polynomial in 4 variables given by

$$\begin{aligned} -(&x_1^3x_2x_3x_4 + x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 \\ &+ x_1x_2^3x_3x_4 + x_1x_2x_3^3x_4 + x_1x_2x_3x_4^3 + x_2^2x_3^2x_4^2). \end{aligned} \tag{51}$$

This time the leading monomial in (51) is the product of x_1^2 with $x_1x_2x_3x_4$, which are the leading terms of s_1^2 and s_4. Accordingly subtracting $-s_1^2s_4$ from (51), we obtain

$$\begin{aligned} &-x_1^2x_2^2x_3^2 + 2x_1^2x_2^2x_3x_4 - x_1^2x_2^2x_4^2 + 2x_1^2x_2x_3^2x_4 + 2x_1^2x_2x_3x_4^2 \\ &\quad - x_1^2x_3^2x_4^2 + 2x_1x_2^2x_3^2x_4 + 2x_1x_2^2x_3x_4^2 + 2x_1x_2x_3^2x_4^2 - x_2^2x_3^2x_4^2. \end{aligned} \tag{52}$$

The leading monomial in (52) is the square of $x_1x_2x_3$. Subtracting $-s_3^2$ from (52), we obtain

$$4x_1^2x_2^2x_3x_4 + 4x_1^2x_2x_3^2x_4 + 4x_1^2x_2x_3x_4^2 + 4x_1x_2^2x_3^2x_4 + 4x_1x_2^2x_3x_4^2 + 4x_1x_2x_3^2x_4^2. \tag{53}$$

Not only does the leading monomial in (53) equals that of s_2s_4, in fact the expression as a whole equals $4s_2s_4$. We conclude that (51) equals $-s_1^2s_4 - s_3^2 + 4s_2s_4$.

(iv) Let $f = x^n + \alpha_1x^{n-1} + \ldots + \alpha_{n-1}x + \alpha_n \in K[x]$, and write

$$f = (x - x_1)\cdots(x - x_n) \in L[x] \tag{54}$$

over a splitting field $L|K$ of f. Then we have

$$\alpha_i = (-1)^i s_i(x_1, \ldots, x_n) \tag{55}$$

for $1 \leq i \leq n$. ❀

By the universal property of the field of fractions, the action of S_n on $R = k[x_1, \ldots, x_n]$ from Proposition 3.1 induces an action of S_n on the rational function field $L = Q(R) = k[x_1, \ldots, x_n]$. We can therefore consider the corresponding fixed field, which is the business of the following corollary.

Corollary 3.5. *Let k be a field, let $L = k(x_1, \ldots, x_n) = Q(k[x_1, \ldots, x_n])$ be a rational function field in $n > 0$ variables over k. Then we have $L^{S_n} = k(s_1, \ldots, s_n)$, and there is a natural isomorphism*

$$\mathrm{Gal}(L|L^{S_n}) \simeq S_n. \tag{56}$$

Proof. The inclusion $k(s_1,\dots,s_n) \subset L$ is a consequence of Theorem 3.3(i). To obtain the reverse inclusion, suppose that $q \in L$ is a rational function invariant under S_n. Let us write $q = f/h$ for $f,h \in k[x_1,\dots,x_n]$ with h non-zero. Let $H = \prod_{\sigma\in S_n} h$. Then since σ permutes the factors that define H, we have

$$H \in k[x_1,\dots,x_n]^{S_n} = k[s_1,\dots,s_n] \subset k(s_1,\dots,s_n). \tag{57}$$

Now since $hq = f$ is an element of $k[x_1,\dots,x_n]$, the same is true for its multiple Hf. Moreover, given $\sigma \in S_n$ we have

$$\sigma(Hq) = \sigma(H)\sigma(q) = Hq \tag{58}$$

where the final equality is a consequence of (57) and our assumption that $q \in L^{S_n}$. Since σ is arbitrary, we see that

$$Hq \in k[x_1,\dots,x_n]^{S_n} = k[s_1,\dots,s_n] \subset k(s_1,\dots,s_n). \tag{59}$$

Combining (57) and (59), we see that

$$q = (Hq)/H \in k(s_1,\dots,s_n); \tag{60}$$

do note that H is non-zero, as it is a product of the images of the non-zero polynomial h under the action of the various elements of S_n.

The definition of the action of S_n implies that no two different permutations in S_n define the same action on L, so that we may consider S_n as a subgroup of $\mathrm{Aut}(L)$. The claim (56) therefore follows from Theorem III.2.3(ii). ♡

Remark 3.6. The proof of Corollary 3.5 is more tricky than might appear to be needed in light of Theorem 3.3; one would hope that is we write $q = f/h$ for f and h coprime, then we would automatically have that f and h are invariant under S_n if the same is true for q. This statement is true, but its proof is somewhat involved; see Exercise 8. ❁

Remark 3.7. One of the first persons to study the theory symmetric polynomials in generality was Joseph-Louis Lagrange (1736-1813), who considered symmetric polynomials in his 1771 work *Réflexions sur la résolution algébrique de s équations*. It was in this context that he observed that the cardinality of the S_n-orbit of a non-symmetric polynomial under the action of S_n divides $n!$, which was an early version of his eponymous theorem in the theory of groups.

Lagrange worked on symmetric polynomials before Galois theory existed in the first place, and also nowadays these polynomials have important applications outside of Galois theory. One example is given by the identities for POWER SUMS, such as the symmetric polynomial

$$f = x_1^3 + x_2^3 + x_3^3 \in \mathbb{Q}[x_1,x_2,x_3]^{S_3}, \tag{61}$$

which can be written as

$$f = s_1^3 - 3s_1s_2 + 3s_3 \in \mathbb{Q}[s_1,s_2,s_3]. \tag{62}$$

Before Lagrange's results, Isaac Newton (1642–1727) had already obtained identities for power sums in terms of symmetric polynomials. These identities lead to so-called fluid solutions to Einstein's field equations, which play a role in current cosmological models. ❁

4 Description: Permutation groups

It is now time to answer Question (ii) from the introduction. The theory of permutation groups will allow us to make Galois groups of a splitting field $f \in K[x]$ especially concrete, since it allows the description of these groups in terms of the permutations of the zeros of f that they induce.

Theorem 4.1. *Let K be a field, let $f \in K[x]$ be a polynomial of degree $n \leq 1$, and let $L|K$ be a splitting field of f, with $Z \subset L$ the set of zeros of f in L. Then the following statements hold.*

(i) We have $\#Z = n$ if and only if f is separable, in which case the extension $L|K$ is finite Galois.

(ii) The permutation action

$$\begin{aligned} \mathrm{Aut}(L|K) &\to \mathrm{Sym}(Z) \\ \sigma &\mapsto (\beta \mapsto \sigma(\beta)) \end{aligned} \tag{63}$$

is FAITHFUL*, in the sense that the only element of $\mathrm{Aut}(L|K)$ that permutes the elements of Z trivially is the identity automorphism.*

(iii) The polynomial f is irreducible if and only if the action from (ii) is TRANSITIVE*, in the sense that given any two zeros β and β' of f there exists a $\sigma \in \mathrm{Aut}(L|K)$ such that $\sigma(\beta) = \beta'$.*

Proof. (i): Since f splits into linear factors over its splitting field L, the first statement follows from the definition of separability. The second follows from Proposition 1.5.

(ii): First note that the action (63) is well-defined by Proposition 1.5. Now if $\sigma \in \mathrm{Aut}(L|K)$ fixes all elements of Z, then it also fixes all elements of the field $K(Z)$, since it is a field homomorphism; see Exercise 4. Since $L = K(Z)$, we see that σ is the identity automorphism of L, so that the claim follows.

(iii): If f is irreducible, then $K(\beta)$ and $K(\beta')$ are both K-isomorphic to $K[x]/(f)$, and the prolongation lemma 1.4 shows that any K-isomorphism $K(\beta) \to K(\beta')$ can be extended to an element of $\mathrm{Aut}(L|K)$. Conversely, if $f = gh$ is a non-trivial factorization in $K[x]$, then $\mathrm{Aut}(L|K)$ maps the set of zeros of g to itself by Proposition 1.5. In particular, no such zero β can be sent to a zero β' of h, and therefore the action is not transitive. ♡

Remark 4.2. (i) The converse to the second part of Theorem 4.1(i) does not hold; see Remark II.2.12 and Exercise 7.

(ii) In practice, one often numbers the zeros of f by fixing a factorization

$$f = (x - \beta_1) \cdots (x - \beta_n) \in L[x]. \tag{64}$$

Considered in this way, Theorem 4.1(ii) shows that $\mathrm{Aut}(L \mid K)$ can be interpreted as a subgroup of the symmetric group S_n. Whether one chooses a specific numbering or not, the concrete interpretation of Theorem 4.1(ii) is that $\mathrm{Aut}(L \mid K)$ can be understood as a group of permutations of the

zeros of the polynomial $f \in K[x]$; in a sense, $\mathrm{Aut}(L|K)$ consists of those permutations of the set of zeros that extend to K-linear automorphisms of the field L. ❁

Definition 4.3. Let $f \in K[x]$ be a separable polynomial of degree n, and let $L|K$ be the splitting field of f. We will occasionally denote the Galois group of the extension $L|K$ by $\mathrm{Gal}(f)$ instead, and identify this group with a subgroup of S_n as in Remark 4.2(ii). ✌

At this point, Galois groups are concrete enough that we can study many examples of them.

Example 4.4. (i) Let K be a field, and let $f \in K[x]$ be a quadratic polynomial, with splitting field $L|K$. If f is **separable**, then Part (i) of Theorem 4.1 shows that $L|K$ is Galois. Part (ii) of the theorem implies that $\mathrm{Gal}(L|K)$ be considered as a subgroup of the symmetric group S_2 on the two zeros of f. Therefore $\mathrm{Gal}(L|K)$ is either trivial or generated by the automorphism that switches the two zeros of f. Part (iii) of the Theorem 4.1 shows that the latter case occurs exactly if f is irreducible. In particular, the polynomials

$$f = x^2 - 2 \in \mathbb{Q}[x] \tag{65}$$

and

$$f = x^2 + x + 1 \in \mathbb{F}_2[x] \tag{66}$$

from Example 1.7(i) both have Galois group $S_2 \simeq C_2$.

If f is **inseparable**, then necessarily $f = (x-\beta)^2$ over $\overline{K}[x]$. Either $\beta \in K$, in which case $L|K$ is the trivial extension, or β is defined over an extension of K. In Example 1.7(i), we have seen that the latter case can only happen if $\mathrm{char}(K) = 2$. In this case f is irreducible as an element of $K[x]$, but $\mathrm{Aut}(L \mid K)$ is still the trivial group, for example because Theorem 4.1 implies that it admits an injective group homomorphism to the symmetric group on a set of cardinality 1. An example of this behavior is provided by the inseparable irreducible polynomial

$$f = x^2 - t \in K[x] \tag{67}$$

over $K = \mathbb{F}_2(t)$.

(ii) Now let $f \in K[x]$ be cubic. Suppose first that f is **separable**, so that the splitting field L of f is Galois over K by Theorem 4.1(i). If f is irreducible, then we are in one of the cases (a1) and (a2) in Example (1.7)(ii). In the former case, the splitting field L of f over K coincides with the stem field of f, and $\mathrm{Gal}(L|K)$ is of order 3, and therefore cyclic; in the latter case, L is of degree 6 over K. Since Theorem 4.1(ii) shows that $\mathrm{Gal}(L|K)$ can be considered as a subgroup of the symmetric group S_3 on the two zeros of f, we see that $\mathrm{Gal}(L|K) \simeq S_3$ in this case.

If f is not irreducible, then there are two other possibilities, depending on the factorization of f into irreducible elements of $K[x]$:

(a3) If $f = \ell q$ with $\ell \in K[x]$ linear and q quadratic and irreducible in $K[x]$, then Part (i) of this Example shows that $\mathrm{Gal}(L|K) \simeq C_2$. Indeed, any element of $\mathrm{Gal}(L\,|\,K)$ has to map the zero of ℓ to itself by Proposition 1.5; on the other hand, the proof of Theorem 4.1(iii) shows that there exists an element of $\mathrm{Gal}(L\,|\,K)$ that switches the zeros of the quadratic polynomial $q \in K[x]$. An example of this case is given by the polynomial

$$f = x(x^2+1) \in \mathbb{Q}[x]. \tag{68}$$

(a4) If $f = \ell_1\ell_2\ell_3$ is a product of distinct linear factors ℓ_i in $K[x]$, then $\mathrm{Gal}(L|K)$ is trivial. Indeed, any element σ of $\mathrm{Gal}(L|K)$ has to map the zeros of ℓ_i to themselves by Proposition 1.5, so that σ fixes the zeros of f and is therefore trivial by Theorem 4.1(ii). An example of this case is given by the polynomial

$$f = x(x^2-1) = x(x-1)(x+1) \in \mathbb{Q}[x]. \tag{69}$$

Now suppose that f is **inseparable**. If f is irreducible, then we are in the case (b1) in Example 1.7(ii). If not, then there are three other possibilities, depending on the factorization of f into irreducible elements of $K[x]$:

(b2) If $f = \ell q$ with $\ell \in K[x]$ linear and q quadratic and irreducible in $K[x]$, then $\mathrm{Aut}(L|K)$ is trivial even though $L|K$ is not. Indeed, any element of $\mathrm{Gal}(L\,|\,K)$ has to map the zero of ℓ to itself by Proposition 1.5, and the same is true for q, which has a unique zero because f is inseparable, so that Theorem 4.1(ii) shows that $\mathrm{Gal}(L|K)$ is trivial. As in Example 1.7(i), we see that this case can only happen if $\mathrm{char}(K) = 2$. An example of this case is given by the polynomial

$$f = x(x^2+t) \in K[x], \tag{70}$$

where $K = \mathbb{F}_2(t)$.

(b3) If $f = \ell_1\ell_2^2$ with $\ell_1, \ell_2 \in K[x]$ linear, then $L = K$ is trivial, and therefore so is $\mathrm{Aut}(L|K)$. Note that in this case $L|K$ is Galois, even though its defining polynomial f is inseparable. This is not in contradiction with Corollary II.2.10, as f is not irreducible in this case; also see Exercise 7. An example of this case is given by the polynomial

$$f = x^2(x-1) \in \mathbb{Q}[x]. \tag{71}$$

(b4) If $f = \ell^3$ with $\ell \in K[x]$ linear, then $L = K$ is trivial, and therefore so is $\mathrm{Aut}(L|K)$. As in the case (b3), we see that $L|K$ is Galois, even though its defining polynomial f is inseparable. An example of this case is given by the polynomial

$$f = x^3 \in \mathbb{Q}[x]. \tag{72}$$

The automorphism group $\mathrm{Aut}(L|K)$ is trivial in all cases (b1)-(b4). This is peculiar to degree 3; the reducible quartic polynomial $f = (x^2+x+1)^2 \in$

$\mathbb{F}_2[x]$ is inseparable, but Part (i) of this Example shows that its splitting field defines the quadratic extension $\mathbb{F}_4$ of $\mathbb{F}_2$.

Regardless, we see that things quickly get unpleasant as we move beyond the case where f is separable and irreducible. So in these notes, we will mostly restrict ourselves to that more comfortable case.

(iii) We now take up the thread from Example 1.7(iii) and consider the separable and irreducible polynomial

$$f = x^4 - 2 \in \mathbb{Q}[x]. \tag{73}$$

We have seen that if we let $\beta = \sqrt[4]{2}$, then the stem field $\mathbb{Q}(\beta)$ is not Galois over $K = \mathbb{Q}$. However, Theorem 4.1 shows that the splitting field L of f is Galois over $\mathbb{Q}$, and that if we number the zeros of f in $\mathbb{C}$ by

$$\beta_1 = \beta = \sqrt[4]{2}, \quad \beta_2 = i\sqrt[4]{2}, \quad \beta_3 = -\sqrt[4]{2}, \quad \beta_4 = -i\sqrt[4]{2}, \tag{74}$$

then $\mathrm{Gal}(L|\mathbb{Q})$ can be identified with a subgroup of S_4.

It remains to be seen which subgroup of S_4 we obtain. For this, we first observe that

$$L := \mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4) = \mathbb{Q}(\beta, i). \tag{75}$$

Indeed, since $\beta = \beta_1$ and $i = \beta_2/\beta_1$, we have $\mathbb{Q}(\beta, i) \subset L$, and the converse inclusion holds because

$$\beta_1 = \beta, \quad \beta_2 = i\beta, \quad \beta_3 = -\beta, \quad \beta_4 = -i\beta. \tag{76}$$

Now let us consider the chain

$$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\beta, i) \tag{77}$$

We have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$ because $f \in \mathbb{Q}[x]$ is irreducible. The minimal polynomial of i over $\mathbb{Q}(\beta)$ is still given by $x^2 + 1$, as this quadratic polynomial cannot have a zero over the real field $\mathbb{Q}(\beta)$. Therefore we see that

$$[\mathbb{Q}(\beta, i) : \mathbb{Q}] = [\mathbb{Q}(\beta, i) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 2 \cdot 4 = 8. \tag{78}$$

Now Exercise 9 (but also see Proposition V.2.1) shows that the only subgroup of S_4 with 8 elements is isomorphic to the dihedral group D_4. This is therefore the Galois group of the extension $L|\mathbb{Q}$.

We can even determine $\mathrm{Gal}(L \mid K)$ as a subgroup of S_4. For example, let us see what permutations in S_4 can be induced by automorphisms $\sigma \in \mathrm{Gal}(L \mid L)$ that send β_1 to β_2. If σ is such an automorphism, then necessarily also

$$\sigma(\beta_3) = \sigma(-\beta_1) = -\sigma(\beta_1) = -\beta_2 = \beta_4. \tag{79}$$

Therefore the sole remaining choice is whether we send β_2 to β_1 or β_3. In the former case we obtain the permutation (1 2)(3 4), and in the latter case

we obtain (1 2 3 4). Reasoning similarly for the other images of β_1, we see that the only possible elements of $\mathrm{Gal}(L|K)$ are

$$\begin{array}{cccc} e, & (2\ 4), & (1\ 2\ 3\ 4), & (1\ 2)(3\ 4), \\ (1\ 3)(2\ 4), & (1\ 3), & (1\ 4\ 3\ 2), & (1\ 4)(2\ 3). \end{array} \tag{80}$$

Since $\#\mathrm{Gal}(L\,|\,K) = 8$, we conclude that (80) describes the elements of $\mathrm{Gal}(L|K)$. Our argument also shows that all these permutations indeed come from an actual automorphism $\sigma \in \mathrm{Gal}(L|K)$, which is by no means obvious a priori.

(iv) A special case of Theorem 4.1 is obtained when $f \in K[x]$ is a separable irreducible polynomial (of degree n say) that splits into linear factors over its stem field $L = K[x]/(f)$. Proposition 1.4 then shows that $L|K$ is Galois, and Theorem 4.1 shows that $\mathrm{Gal}(L|K)$ can be considered as a transitive subgroup of S_n with n elements.

It is tempting to conclude that this case always leads to a cyclic Galois group. While this is possible, for example when $K = \mathbb{Q}(i)$ and

$$f = x^4 - 2 \in K[x], \tag{81}$$

(see Exercise 10), this is not always true. A counterexample is given by the polynomial

$$f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x], \tag{82}$$

which factors over $\mathbb{C}$ as

$$f = (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \in \mathbb{C}[x]. \tag{83}$$

More precisely, f is the minimal polynomial over $\mathbb{Q}$ of the element $\beta = \sqrt{2} + \sqrt{3}$, and we have

$$L := \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \tag{84}$$

(see Exercise 11). In particular, L is Galois over $\mathbb{Q}$, since it is equally well the splitting field of the non-irreducible polynomial

$$g = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]. \tag{85}$$

Now we observe that an automorphism $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ of the quartic Galois extension $L|\mathbb{Q}$ is determined by where it maps $\sqrt{2}$ and $\sqrt{3}$, which leads 2 choices in either case. If we number the zeros of g by

$$\gamma_1 = \sqrt{2}, \quad \gamma_2 = -\sqrt{2}, \quad \gamma_3 = \sqrt{3}, \quad \gamma_4 = -\sqrt{3}, \tag{86}$$

then this leads to 4 possible elements of S_4, namely

$$e, \quad (1\ 2), \quad (3\ 4), \quad (1\ 2)(3\ 4). \tag{87}$$

Together, these elements generate a subgroup of S_4 that is isomorphic to the Vierergruppe V_4. Said subgroup is not transitive, but this is because

we changed the defining polynomial of L to g; using f instead, we obtain the 4 permutations

$$e, \quad (1\ 2)(3\ 4), \quad (1\ 3)(2\ 4), \quad (1\ 4)(2\ 3), \tag{88}$$

regardless of how we number the zeros of f; see Exercise 12. ❀

Theorem 4.1(ii) has the considerable advantage that it makes the composing two automorphisms in $\mathrm{Aut}(L \mid K)$ easier to describe, as it corresponds to the composition of permutations in $\mathrm{Sym}(Z)$. More complete and systematic methods to determine Galois groups by means of this theorem will be discussed in Chapters V and VII.

Remark 4.5. Much of what happened in the life of Évariste Galois (1811–1832), the inventor of the theory developed in these notes, is still unclear. What is agreed upon is that he died after having been shot in the abdomen during a duel. It is not known for sure who shot Galois, and the motives are murky beyond his own claim that "Je meurs victime d'une infâme coquette". Galois was not exactly a choirboy and like Alexandre Dumas père, the author of the immortal classic *Le Comte de Monte Cristo*, who knew him personally, he was a convinced republican; for this reason, he refused the last rites, and his funeral culminated in a riot.

An extra layer of fascination around the story of Galois' life is provided by the myths that were actively developed about his achievements, which emphasize his brilliance to the point of absurdity, claiming that Galois wrote all of his main mathematical ideas down in the single night before the final duel. This historiography is analyzed in Rothman's article [Rot], which is recommended reading. Despite these unscientific, genius-worshipping exaggerations, the fact remains that Galois had developed his transformative ideas by the age of 20, which is in itself already more than enough to lead many mathematicans to develop a case of the imposter syndrome. A modern edition of his work can be found in [Gal89].

Galois wrote down his first results on polynomial equations and their Galois groups in two papers that he submitted to the Académie des Sciences in 1829. Their referee Augustin-Louis Cauchy (1789–1857) did not recommend them for acceptance, perhaps because he considered them to be prize-worthy entries for prestigious competitions. Later Galois discovered that some of his results had already been proved by Nils Henrik Abel (1802–1829), so he resubmitted this work in 1830 under the title *Mémoire sur les conditions de résolubilité des équations par radicaux*. This paper was deemed of such high quality that it was forwarded to Jean-Baptiste Joseph Fourier for the Grand Prix of the Académie, since he was its secretary. However, Fourier died that year, which caused Galois' work to be lost. As Galois discovered, that year's prize would be awarded to Abel and Jacobi instead.[1] His work was never considered or mentioned during his lifetime, and it was first published in 1846 afer his death by Joseph Liouville (1809–1882).

[1] See https://en.wikipedia.org/wiki/Galois#Budding_mathematician [Accessed 16 May 2024]

In the aforementioned *Mémoire* [Gal89], Galois defines his eponymous group in the following way:

"Soit une équation donnée, dont a, b, c, ... sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, ... qui jouira de la propriété suivante:

1° Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue;

2° Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions."

This is basically the point of view from Section 2. In Remark IV.1.4, we shall discuss Galois' own formulation of his most famous theorem. ❁

5 Exercises for Chapter III

Exercise 1. Let $L|K$ be a finite Galois extension. Show that L is the splitting field of a separable polynomial $f \in K[x]$. (In fact one can even prove that f can be chosen to be irreducible as well; see Remark IV.4.2(iv).)

Exercise 2. Let $L = K(\beta_1, \ldots, \beta_n)$ be a finitely generated algebraic extension. Show that the following statements are equivalent.

(i) $L|K$ is Galois.

(ii) The minimal polynomials of the elements $\beta_1, \ldots, \beta_n$ are separable and split into linear factors in $L[x]$.

Exercise 3. Generalize Theorem I.2.1 by proving that a field extension $L|K$ of finite degree is Galois if and only if it is the splitting field of a separable polynomial $f \in K[x]$.

Exercise 4. Show that the set L^G defined in (26) is indeed a field. Moreover, show that if $Z \subset L^G$, then also $K(Z) \subset L^G$.

Exercise 5. Let $L|K$ and $L'|K$ be field extensions, and let $\sigma, \sigma' : L \to L'$ be two K-homomorphisms. Suppose that $S \subset L$ is such that $L = K(S)$. Show that $\sigma = \sigma'$ if and only if $\sigma(\beta) = \sigma'(\beta)$ for all $\beta \in S$.

Exercise 6. Let $L|K$ be an extension, and let $G \subset \mathrm{Aut}(L|K)$ be a finite subgroup. Suppose that a black box provides us with the conclusion that $[L : L^G] = \#G$. Show that $L|L^G$ is normal and separable (without using the direct argument from the proof Theorem 2.3).

Exercise 7. Let K be a field, and let $f \in K[x]$ be a polynomial with splitting field $L|K$. Show that L may be Galois even if f is inseparable.

Exercise 8. Let k be a field, let $n > 0$, and consider the symmetric group S_n acting on $R = k[x_1, \ldots, x_n]$ and $L = k(x_1, \ldots, x_n)$ as in Proposition 3.1.

(i) Show that the only non-trivial homomorphism $S_n \to k^*$ is given by the sign homomorphism.

(ii) Let $q \in L^{S_n}$, and write $q = f/g$ for coprime polynomials $f, g \in k[x_1, \ldots, x_n]$. Show that there exist unique group homomorphisms $\sigma_f, \sigma_g : S_n \to k^*$ such that $\sigma(f) = s_f(\sigma)f$ and $\sigma(g) = s_g(\sigma)f$ for all $\sigma \in S_n$.

(iii) Show that if s_f is non-trivial, then $f = Df_0$, where D is the discriminant polynomial from Proposition 1.6 and where $f_0 \in R^{S_n}$.

(iv) Prove that the polynomials f and g from (ii) are indeed symmetric.

Exercise 9. Let $G \subset S_4$ be a subgroup of cardinality 8. Show that G is isomorphic to the dihedral group D_4.

Exercise 10. Show that the polynomial in (81) has a Galois group that is cyclic of order 4.

Exercise 11. Prove the factorization in (83), and show that $f = x^4 - 10x^2 + 1$ is indeed the minimal polynomial of $\beta = \sqrt{2} + \sqrt{3}$. (Hint: Show that $\mathbb{Q}(\beta)$ contains all of the square roots $\sqrt{6}$, $\sqrt{2}$, and $\sqrt{3}$.)

Exercise 12. Prove the final statement of Example 4.4(iv).

Exercise 13. For each of the following pairs K and f, determine whether the irreducible polynomial f defines a Galois extension of K, and determine the corresponding Galois group if it does.

(i) $K = \mathbb{Q}$, $f = x^3 - 2$.

(ii) $K = \mathbb{Q}(\sqrt{3})$, $f = x^3 - 2$.

(iii) $K = \mathbb{Q}(\sqrt{-3})$, $f = x^3 - 2$.

(iv) $K = \mathbb{F}_3$, $f = x^3 - x - 1$.

(v) $K = \mathbb{Q}$, $f = x^4 + 5$.

(vi) $K = \mathbb{Q}$, $f = x^4 + x^3 + x^2 + x + 1$.

(vii) $K = \mathbb{Q}$, $f = x^4 - x^2 + 1$.

Exercise 14. For devout non-believers: State and prove all the results in this chapter without making use of an algebraic closure.

Summary and main notions of the chapter

With the notions in this chapter, we can phrase the answers to the Questions (i) and (ii) in its introduction as follows:

(i) Theorem 1.2 shows that the finite extensions $L|K$ with "maximal" automorphism groups are exactly those for which $\#\mathrm{Aut}(L|K) = [L : K]$. Such finite extensions are called Galois extensions, and they are the main topic of study of these notes.

Finite Galois extensions can be characterized in two ways: Either as normal and separable extensions of the base field K (Theorem 1.2) or as subfields of L obtained as the fixed field of a finite group of automorphisms (Theorem 2.3).

(ii) When $L|K$ is a splitting field of a separable polynomial $f \in K[x]$, Theorem 4.1 shows that the Galois group $\mathrm{Gal}(f) = \mathrm{Gal}(L|K)$ can be studied in terms of the permutations of the zeros of f that its elements induce.

The key skills to take away from this are the following:

– Given a finite extension $L|K$, you can determine whether it is a Galois extension by means of the explicit criteria from the previous chapters for such an extension to be normal and separable; see Propositions 1.4 and 1.5.

– You are aware of the alternative description of Galois extensions by means of fixed fields provided in Corollary 2.7, and you can determine the minimal polynomials of elements of Galois extensions by means of this characterization (Corollary 2.5). Moreover, you are able to rewrite symmetric polynomials as expressions in elementary symmetric polynomials (Theorem 3.3 and Example 3.4).

– For splitting fields of separable polynomials, you know the concrete description of the corresponding Galois group provided by Theorem 4.1, and you can use this in some simple cases to determine said group; see Example 4.4.

Chapter IV

The main theory of Galois theory

We can now formulate the one astonishing result that is the centerpiece of Galois theory. This result is an explicit correspondence between the subgroups

$$H \subset \mathrm{Gal}(L|K) \tag{1}$$

of the automorphism group $\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K)$ of a finite Galois extension and the intermediate subfields

$$K \subset M \subset L \tag{2}$$

of the field extension $L|K$. This main theorem of Galois theory is not only interesting in itself, but it has also been an important tool for the study of algebraic and geometric questions. This usefulness continues until the present day, and is likely to last until Galois theory is subsumed by an even more elegant theory, if such a thing is possible. Many historical and practical applications will be considered in Chapter VI; in the present chapter, we already briefly mention how the primitive element theorem be obtained as one of its corollaries.

The proof of the main theorem is surprisingly quick, but part of its subtlety lies in understanding what it actually does, namely to provide a translation of field-theoretic problems into group theory and conversely. To understand this connection, we in particular have to be able to provide a solid and convincing answer to the following questions:

(i) Let $H \subset \mathrm{Gal}(L|K)$ be a subgroup. How can we associate a subextension $M|K$ of $L|K$ to H in a natural way?

(ii) Let $M|K$ be a subextension of $L|K$. How can we associate a subgroup $H \subset \mathrm{Gal}(L|K)$ to $M|K$ in a natural way?

(iii) How are the group-theoretic properties of a subgroup $H \subset \mathrm{Gal}(L|K)$ related to the field-theoretic properties of the corresponding subextension $M|K$ of $L|K$?

An answer to these questions is provided by the contruction of the FIXED FIELD of a group of automorphisms H, as well as the FIX GROUP of a subextension $M|K$. These associations will provide the grammar for the aforementioned

translation, after which the estimates from Chapter III allows us to prove the main theorem, which simply states that the two associations in (i) and (ii) are mutually inverse. After this, we shall also be able what effect changing either of the fields L or K has on the corresponding group $\mathrm{Gal}(L|K)$. In particular, we shall be able to prove in Theorem 2.3 that a subextension $M|K$ of $L|K$ is normal in the sense of Chapter I if and only if the corresponding fix group is a normal subgroup of $\mathrm{Gal}(L|K)$.

We might as well jump in straight away, especially since the answers to Questions (i) and (ii) above are, at least conceptually, as pleasant as they could possibly be.

1 The Galois correspondence

We have in fact already seen the answer to Question (i) in Definition III.2.1: Given an extension $L|K$ along with a subgroup H of $\mathrm{Aut}(L|K)$, we have constructed the FIXED FIELD

$$L^G = \{\beta \in L \,:\, \sigma(\beta) = \beta \text{ for all } \beta \in G\}. \tag{3}$$

To answer Question (ii), we need a new definition.

Definition 1.1. Let $M|K$ be a subextension of a field extension $L|K$, so that $K \subset M \subset L$. Then we define the FIX GROUP of $M|K$ to be the subgroup

$$\mathrm{Aut}(L|M) = \{\sigma \in \mathrm{Aut}(L|K) \,|\, \sigma_M = \mathrm{id}_M\} \tag{4}$$

of $\mathrm{Aut}(L|K)$. ✌

By Exercise 1, the fix group $\mathrm{Aut}(L|M)$ is indeed a subgroup of $\mathrm{Aut}(L|K)$. We can now state Galois' main result, which describes a precise relation between subgroups of $\mathrm{Gal}(L|K)$ and subextensions of $L|K$.

Theorem 1.2 (Main theorem of Galois theory)**.** *Let $L|K$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(L|K)$. Then the following statements hold.*

(i) The maps of sets

$$\begin{aligned} \{\textit{Subgroups of } G\} &\leftrightarrow \{\textit{Subextensions of } L|K\} \\ H &\mapsto L^G \\ \mathrm{Aut}(L|M) &\hookleftarrow M \end{aligned} \tag{5}$$

are mutually inverse.

(ii) Let H and H' be subgroups of G, with corresponding intermediate extensions $M|K$ and $M'|K$. Then

$$H \subset H' \quad \textit{if and only if} \quad M \supset M'. \tag{6}$$

(iii) Given a subgroup $H \subset \mathrm{Gal}(L|K)$, we have

$$[L : L^H] = \#H \quad \textit{and} \quad [L^H : K] = [G : H]. \tag{7}$$

Proof. (i): The fact that the indicated maps are mutually inverse reduces to the statements that

$$\mathrm{Aut}(L|L^H) = H \quad \text{for every subgroup } H \text{ of } G \tag{8}$$

and

$$L^{\mathrm{Aut}(L|M)} = M \quad \text{for every subextension } M|K \text{ of } L|K. \tag{9}$$

The first of these statements is a rephrasing of Theorem III.2.3(i), whereas the second rephrases Part (ii) of the same theorem.

(ii): If $H \subset H'$, then any element of L that is fixed by H' is necessarily fixed by its subgroup H, meaning that

$$M' = L^{H'} \subset L^H = M. \tag{10}$$

Conversely, if $M' \subset M$, then any automorphism of L that fixes M necessarily fixes its subfield M', so that $H \subset H'$.

(iii): Corollary III.2.7 shows that $L|L^H$ is a Galois extension, so that $\#\mathrm{Aut}(L|L^H) = [L : L^H]$. Moreover, the same result shows that $\mathrm{Aut}(L|L^H) = H$, so that in fact $[L : L^H] = \#H$. This proves the first statement, which implies the second as the tower law yields the first equality in the chain

$$[L^H : K] = [L : K]/[L : L^H] = \#G/\#H = \#[G : H]. \tag{11}$$

♡

Example 1.3. (i) Let $L|K$ be a separable quadratic extension. Then Example III.4.4(i) shows that $G = \mathrm{Gal}(L|K) \simeq C_2$. This group admits only two subgroups, namely itself and the trivial subgroup. Because of Part (ii) of Theorem 1.2, we see that the trivial subgroup $\{e\}$ corresponds to the full extension $L|K$, whereas the full group G corresponds to the trivial subextension $K|K$.

(ii) Similarly, suppose that $f \in K[x]$ is a separable irreducible cubic polynomial that splits into linear factors over its stem field $L = K[x]/(f)$. Then Example III.4.4(ii) shows that $G = \mathrm{Gal}(L|K) \simeq C_3$. This group once again admits only two subgroups, which correspond to $L|K$ and $K|K$, respectively.

Once again we see that $L|K$ has no proper subextensions beside the trivial subextension $K|K$. This fact can also be deduced by means of the tower law.

(iii) Now let $K = \mathbb{Q}$, and let L be the splitting field of the irreducible polynomial $f = x^3 - 2 \in \mathbb{Q}[x]$. In Example 4.4(ii), we have shown that numbering the roots of f in $\mathbb{C}$ gives rise to an identification of $\mathrm{Gal}(L|K)$ with S_3. We choose the numbering

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3\sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2\sqrt[3]{2}. \tag{12}$$

The group G has 6 subgroups H in total, and we will now determine the corresponding subextensions L^H of $L|K$.

H = {e}: Since all elements of L are fixed by the trivial automorphism, we get $L^H = L$ in this case.

H = S₃: Since S_3 is its largest among the subgroups of G, the extension $L^{S_3}|K$ is the smallest among the subextensions of $L|K$ by Theorem 1.2(ii). It therefore corresponds with the minimal subextension $K|K$ of $L|K$. Alternatively, this follows from Theorem III.2.3(ii).

H = ⟨(1 2)⟩: By construction, the zero α_3 of f is fixed by H. Therefore $L^H \supset \mathbb{Q}(\alpha_3)$. On the other hand, Theorem 1.2(iii) shows that $[L^H : \mathbb{Q}] = 3$. Since we also have $[\mathbb{Q}(\alpha_3) : \mathbb{Q}] = 3$ as f is irreducible in $\mathbb{Q}[x]$, we see that $L = \mathbb{Q}(\alpha_3)$ by the tower law.

H = ⟨(1 3)⟩: Arguing as in the case $H = \langle(1\ 2)\rangle$, we obtain that $L^H = \mathbb{Q}(\alpha_2)$.

H = ⟨(2 3)⟩: Arguing as in the case $H = \langle(1\ 2)\rangle$, we obtain that $L^H = \mathbb{Q}(\alpha_1)$.

H = ⟨(1 2 3)⟩: In this case H is the unique subgroup of G of index 2. Theorem 1.2(iii) shows that $[L^H : \mathbb{Q}] = 2$, and Theorem 1.2(i) then implies that $L^H|\mathbb{Q}$ is the unique quadratic subextension of $L|\mathbb{Q}$. It therefore suffices to find any quadratic subextension of $L|\mathbb{Q}$, as it must then equal $L^H|\mathbb{Q}$. Now $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ contains the imaginary element $\alpha_2/\alpha_1 = \zeta_3$, which defines a quadratic extension of $\mathbb{Q}$ as its minimal polynomial over that field is given by $(x^3 - 1)/(x - 1) = x^2 + x + 1$. We therefore see that $L^H = \mathbb{Q}(\zeta_3)$.

The final entry in the correspondence was obtained in quite an ad hoc way. We will see a more systematic construction in Theorem V.1.7. ❀

Remark 1.4. The bijective correspondence in Theorem 1.2 is called the GALOIS CORRESPONDENCE. It is the central result and essence of Galois theory, as most of its other results can be proved by means of it. Already the result that any Galois extension $L|K$ only has finitely many subextensions is far from obvious (also see Exercise 2); it amounts to the statement that almost none of the in general infinitely many K-subvector spaces of L are also subfields of L.

In Galois' *Mémoire* [Gal89], the Galois correspondence appears in the following way:

"Si l'on adjoint à une équation la valeur *numérique* d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable."

This essentially amounts to the Galois correspondence for the subgroups $S^G(i)$ of G considered in Exercise 3. However, by means of the primitive element theorem 4.1, this allows one to deal with arbitrary subgroups of G by means of the action $G \to \mathrm{Sym}(G/H)$, a fact of which Galois was well aware.

It took a very long time for the broader mathematical world to understand the importance of Galois' work after his death.[1]. Camille Jordan (1838–1922) was one of the first to grasp its essence, and it gradually made its way into the mainstream of mathematics via texts by Heinrich Martin Weber (1842–1913) and Emil Artin (1898–1962). The latter wrote the gem of concision that is the

[1] See https://en.wikipedia.org/wiki/Galois_theory#Aftermath [Accessed 16 May 2024]

classical work [Art98]. These days, Galois theory, invariance, and the application of group theory in algebraic and geometric contexts is an indispensable part of modern mathematics, as we shall see in Chapter VI. It has also continued to inspire mathematicians in modern times. Quoth Michael Harris, referring to Grothendieck's Galois theory (see Remark 3.7(ii)) and the Langlands program (see Section VI.4) in *Mathematics without apologies* [Har15]: "Langlands and Grothendieck are both (at least) Giants by any measure, and both were consciously successors of Galois." In this sense, Galois' vision has triumphed at long last. ❀

2 Subextensions that are Galois

Theorem 1.2 is somewhat asymmetric, as we did not formulate a version of Part (ii) for the automorphism groups of subextensions. The reason for this is somewhat subtle. On the one hand, we have the following statement.

Proposition 2.1. *Let $M|K$ be a subextension of a Galois extension $L|K$. Then $L|M$ is also a Galois extension.*

Proof. By Theorem 1.2(i), we have $M = L^H$ for some subgroup H of $\mathrm{Aut}(L|K)$, and Corollary III.2.7 shows that $L|L^H$ is indeed Galois. (Alternatively, one can show this statement by combining Exercises I.11 and II.4.) ♡

The question whether the subextension $M|K$ is itself Galois is more subtle, and in general this is not the case.

Example 2.2. Let us consider the field extension $L|K$ from Example 1.3(iii). Then the subextension $\mathbb{Q}(\alpha_1)|\mathbb{Q}$ of $L|\mathbb{Q}$ is not Galois. Indeed, if it were, then it would in particular be normal, so that it would contain all zeros $\alpha_1, \alpha_2, \alpha_3$ by Definition I.1.1 and therefore be the full sextic extension $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ which is not the case.

Similarly, the subfields $\mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\alpha_3)$ of L are not Galois. On the other hand, Example 1.3(i) shows that the quadratic subextension $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ of $L|\mathbb{Q}$ is Galois. ❀

Exercise II.4 shows that the subextension $M|K$ is always separable; it is its normality that is the issue. Now the whole philosophy of Galois theory that any statement on Galois extensions and their subextensions can be understood on the level of groups. This case is no exception. In Example 2.2, if we look at the subgroups

$$\langle (2\ 3) \rangle \leftrightarrow \mathbb{Q}(\alpha_1) \qquad \langle (1\ 3) \rangle \leftrightarrow \mathbb{Q}(\alpha_2) \qquad \langle (1\ 2) \rangle \leftrightarrow \mathbb{Q}(\alpha_3) \tag{13}$$

of $\mathrm{Gal}(L|K) = S_3$ that correspond to the cubic subextensions $\mathbb{Q}(\alpha_i)|\mathbb{Q}$, then we see that these subgroups are not normal in S_3. By contrast, the subgroup

$$A_3 = \langle (1\ 2\ 3) \rangle \leftrightarrow \mathbb{Q}(\zeta_3) \tag{14}$$

that corresponds to the quadratic subextension $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ is a normal subgroup of S_3, and said extension is normal because we showed it to be Galois.

At this point, the terminology makes it extremely tempting to suspect that normal subextensions of a Galois extension $L|K$ are exactly those subextensions that correspond to normal subgroups of the Galois group $\mathrm{Gal}(L\,|\,K)$. This suspicion is correct.

Theorem 2.3. *Let $L|K$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(L|K)$, and let $M|K$ be a subextension, with corresponding subgroup $H = \mathrm{Gal}(L|M)$. Then the following statements are equivalent.*

(i) The extension $M|K$ is Galois.

(ii) The extension $M|K$ is normal.

(iii) H is a normal subgroup of G.

If any of these conditions is satisfied, then there exists a canonical isomorphism

$$\begin{aligned} G/H &\xrightarrow{\sim} \mathrm{Aut}(M|K) \\ \sigma H &\mapsto \sigma|_M. \end{aligned} \tag{15}$$

Proof. (i) $\Leftrightarrow$ (ii): Since by definition a field extension is Galois if and only if it is normal and separable, this equivalence is a consequence of Exercise II.4.

(ii) $\Leftrightarrow$ (iii): Let us choose some privileged K-homomorphism of L into $\overline{K}$ and identify L with a subfield of $\overline{K}$ accordingly. Moreover, suppose that $\varphi : M \to \overline{K}$ is a K-homomorphism. We will analyze the normality of $M|K$ by studying what the possible images $\varphi(M)$ are.

Using the prolongation lemma 1.4, we can extend φ to a K-homomorphism $L \to \overline{K}$, which we will denote by σ. Since $L|K$ is a normal extension, we have $\sigma(L) = L$ by Theorem 1.10. In this way, we can consider σ as a K-homomorphism $\sigma : L \to L$. Let us do so. As σ is a K-homomorphism, it is injective, so that it is surjective by the finite-dimensionality of $L|K$ (also see Exercise I.3 for a more general version of this argument).

We conclude that the various K-homomorphisms $M \to L$ are obtained by the restriction of elements $\sigma : L \to L$ in $\mathrm{Aut}(L\,|\,K) = G$. In particular, the various images of M under these K-homomorphisms are given by $\sigma(M)$, where σ runs through G. Moreover, if $H = \mathrm{Aut}(L|M)$ is the fix group of the subfield M, then

$$\mathrm{Aut}(L|\sigma(M)) = \sigma H \sigma^{-1}. \tag{16}$$

This equality a consequence of a general statement on stabilizers of different elements in the orbit under a group action. For more ad hoc proof, let us first suppose that $\tau \in H$, and let $\sigma\beta$ be an element of the image $\sigma(M)$. Then

$$(\sigma\tau\sigma^{-1})(\sigma(\beta)) = \sigma(\tau(\sigma^{-1}(\sigma(\beta)))) = \sigma(\tau(\beta)) \overset{\tau\in H}{=} \sigma(\beta). \tag{17}$$

Since $\beta \in L$ and $\sigma \in H$ were arbitrary, this implies that $\sigma H \sigma^{-1} \subset \mathrm{Aut}(L|\sigma(M))$. Conversely, if $\tau \in \mathrm{Aut}(L|\sigma(M))$, and $\beta \in M$, then

$$(\sigma^{-1}\tau\sigma)(\beta) = \sigma^{-1}(\tau(\sigma(\beta))) \overset{\tau\in\mathrm{Aut}(L|\sigma(M))}{=} \sigma^{-1}(\sigma(\beta)) = \beta \tag{18}$$

for all $\beta \in L$. We see that $\sigma^{-1}\tau\sigma \in \mathrm{Aut}(L\,|\,M) = H$, so that conjugation with σ implies that $\tau \in \sigma H \sigma^{-1}$. Since $\tau \in \mathrm{Aut}(L\,|\,\sigma(M))$ was arbitrary, this implies the converse inclusion $\mathrm{Aut}(L\,|\,\sigma(M)) \subset \sigma H \sigma^{-1}$. We have therefore shown our claim.

Now $M\,|\,K$ is normal if and only if $\sigma(M) = M$ for all $\sigma \in G$. Because the correspondence in Theorem 1.2(i) is bijective, Equation (16) shows that this is the case if and only if $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, and this happens if and only if H is a normal subgroup of G.

If H is indeed normal in G, then the first part of the proof of the equivalence between Parts (ii) and (iii) shows that the map

$$\begin{aligned} G &\xrightarrow{\sim} \mathrm{Aut}(M\,|\,K) \\ \sigma &\mapsto \sigma|_M. \end{aligned} \tag{19}$$

is a well-defined surjective group homomorphism. Its kernel is given by the automorphisms of L that restrict to the identity on M, that is, by $\mathrm{Aut}(L\,|\,M) = H$. The final statement of the theorem then follows from Noether's isomorphism theorem. ♡

Remark 2.4. Galois did not have the terminological epiphany in the discussion before Theorem 2.3 at his disposal; it was of course set up only after his results. He was, however, one of the first mathematicians to see the use of the notion of a normal subgroup. Galois stated the normality of a subgroup H of a group G be saying that the decomposition of G into H-cosets was PROPER, by which he meant that the decomposition of G into left H-cosets coincides with that into right H-cosets. As you will have seen, this is one of the possible definitions of a normal subgroup. ❁

Example 2.5. (i) Let $K = \mathbb{Q}$. For the splitting field $L\,|\,\mathbb{Q}$ of the polynomial $f = x^3 - 2$ from Example 2.2, we see that besides L and $\mathbb{Q}$ itself, the only Galois subextension of $L\,|\,\mathbb{Q}$ is given by $M = \mathbb{Q}(\zeta_3)$, in which case the Galois group is C_2 by Example III.4.4(i).

This is exactly as predicted by Theorem 2.3. Indeed, as we have also seen in Example 1.3(iii), the Galois group $\mathrm{Gal}(L\,|\,\mathbb{Q})$ is isomorphic to S_3, and this group has only a single non-trivial proper normal subgroup, to wit A_3. This group corresponds to the subextension $\mathbb{Q}(\zeta_3)\,|\,\mathbb{Q}$ whose Galois group C_2 is indeed isomorphic to S_3/A_3.

(ii) Let $K = \mathbb{Q}$, and let L be the splitting field of the quartic polynomial $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. In Example III.4.4(iv), we have shown that $G = \mathrm{Gal}(L\,|\,K)$ is isomorphic to the Vierergruppe V_4. This subgroup has exactly three non-trivial proper subgroups H_1, H_2, and H_3, which are generated by its three elements σ_1, σ_2, and σ_3 of order 2. If we describe these elements as in III.(87), then we see that $\sigma_1 = (1\ 2)$ is the stabilizer of both 3 and 4 in G, so that Exercise 3 implies that

$$L^{H_1} = \mathbb{Q}(\gamma_3) = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(-\sqrt{3}) = \mathbb{Q}(\gamma_4). \tag{20}$$

Similarly, we see that for $\sigma_2 = (3\ 4)$ we obtain the fixed field

$$L^{H_2} = \mathbb{Q}(\gamma_1) = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\gamma_2). \tag{21}$$

There is one remaining quadratic subfield of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which therefore has to be $\mathbb{Q}(\sqrt{6})$ since $\sqrt{6} \in L$ and $\sqrt{6}$ is fixed by neither of the automorphisms σ_1 and σ_2. Indeed, σ_1 cannot fix both $\sqrt{2}$ and $\sqrt{3}$, since then we would have $L^{H_1} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = L$, in contradiction with the bijectivity of the Galois correspondence in Theorem 1.2(i). Since σ_1 does fix $\sqrt{3}$, it has send $\sqrt{2}$ to the other zero $-\sqrt{2}$ of its minimal polynomial $x^2 - 2$ over $\mathbb{Q}$ by Proposition I.1.5. Therefore we see that

$$\sigma_1(\sqrt{6}) = \sigma_1(\sqrt{2}\sqrt{3}) = \sigma_1(\sqrt{2})\sigma_1(\sqrt{3}) = -\sqrt{2}\sqrt{3} = -\sqrt{6}. \tag{22}$$

Similarly, we see that

$$\sigma_2(\sqrt{6}) = \sigma_2(\sqrt{2}\sqrt{3}) = \sigma_2(\sqrt{2})\sigma_2(\sqrt{3}) = \sqrt{2}(-\sqrt{3}) = -\sqrt{6}. \tag{23}$$

Since $\sigma_3 = \sigma_1\sigma_2$, we also have

$$\sigma_3(\sqrt{6}) = \sigma_3(\sqrt{6}) = \sigma_3(\sqrt{2})\sigma_3(\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}. \tag{24}$$

Since $H_3 = \langle \sigma_3 \rangle$ is of index 2 in G, Theorem 1.2(iii) shows that L^{H_3} is a quadratic extension of $\mathbb{Q}$. Since it contains the quadratic number field $\mathbb{Q}(\sqrt{6})$ by (24), we conclude that

$$L^{H_3} = \mathbb{Q}(\sqrt{6}). \tag{25}$$

Note that the three fixed fields that we obtained were all quadratic, and therefore all Galois by Example 1.3(i). This makes sense; since V_4 is an abelian group, all its subgroups are normal, which implies that all subextensions of $L|K$ are Galois in light of Theorem 2.3.

❀

Remark 2.6. Another way to prove that γ generates the fixed field L^{H_2} in Example 2.5(ii) is to determine the polynomial

$$f = (x - \gamma)(x - r(\gamma))(x - r^2(\gamma))(x - r^3(\gamma)) \in K[x] \tag{26}$$

by using the theory of symmetric polynomials from Section III.3 and then to check that f is irreducible. While this is in fact the correct general method, and leads to the same minimal polynomial f of γ, it is far too laborious in our particular case. ❀

We now consider a more extended example.

Example 2.7. Let $K = \mathbb{Q}$, and let L be the splitting field of the quartic polynomial $f = x^4 - 2 \in \mathbb{Q}[x]$. In Example III.4.4(iii), we have shown that $G = \mathrm{Gal}(L|K)$ is isomorphic to D_4. Let r and s be the standard generators of D_4. Using the numbering of the zeros in III.(80), we have $D_4 = \langle r, s \rangle$ for

$$r = (1\ 2\ 3\ 4) \quad \text{and} \quad s = (1\ 2)(3\ 4). \tag{27}$$

We can study D_4 by means of its normal subgroup

$$D_4^+ = \langle r \rangle \simeq C_4. \tag{28}$$

If $H \subset D_4$ be a subgroup. Then $H^+ = H \cap D_4^+$ is a subgroup of the cyclic group $D_4^+ = \langle r \rangle$, and there exists a canonical injective homomorphism

$$\begin{aligned} H/H^+ &\to D_4/D_4^+ \simeq C_2 \\ hH^+ &\mapsto hD_4^+, \end{aligned} \tag{29}$$

so that H/H^+ is a cyclic group whose order equals either 1 or 2. Now we have

$$\#H = \#(H/H^+)\#H^+. \tag{30}$$

We use H^+ and H/H^+ to determine the possibilities for H, as follows.

– $\mathbf{H^+ = \{e\}, \#(H/H^+) = 1}$: In this case $H = H^+ = \{e\}$ and

$$L^H = L. \tag{31}$$

This is still a Galois extension of K, in line with the fact that the trivial subgroup of a group is always normal.

– $\mathbf{H^+ = \{e\}, \#(H/H^+) = 2}$: In this case H is generated by an element $g \in G$ of order 2 such that $g \notin \langle r \rangle$. Such an element g is of the form $r^i s$ for some i with $0 \le i \le 3$. Using the numbering in III.(80), these elements are given by

$$g_1 = (1\ 3), \quad g_1' = (2\ 4), \quad g_2 = (1\ 2)(3\ 4), \quad \text{and} \quad g_2' = (1\ 4)(2\ 3). \tag{32}$$

The subgroup $H_1 = \langle g_1 \rangle$ is exactly the stabilizer of 2 and 4 in G and therefore corresponds to the subfield $\mathbb{Q}(\beta_2) = \mathbb{Q}(\beta_4)$; see Exercise 3. Similarly, the fixed field of $H_1' = \langle g_1' \rangle$ is given by $\mathbb{Q}(\beta_1) = \mathbb{Q}(\beta_3)$.

These two fixed fields

$$L^{H_1} = \mathbb{Q}(i\sqrt[4]{2}) \quad \text{and} \quad L^{H_1'} = \mathbb{Q}(\sqrt[4]{2}) \tag{33}$$

are in fact isomorphic. This can be seen because we have $\mathbb{Q}(\beta_i) \simeq \mathbb{Q}[x]/(f)$ for any zero of the irreducible polynomial f, but since the whole philosophy underlying Galois theory promises us that this isomorphism can also be understood by means of group theory alone, we try an alternative approach instead.

The proof of Theorem (16) implies that two subextensions are isomorphic if and only if the corresponding fix groups are conjugate; also see Exercise 5(i). Now stabilizers under a transitive group action, such as that of G on $\{1, 2, 3, 4\}$, are always conjugate. More concretely, this conjugacy in G of the groups H_1 and H_1' follows from the observation that $g_1' = r g_1 r^{-1}$. Also note that this shows that neither of these fields L^{H_1} and $L^{H_1'}$ is Galois over $\mathbb{Q}$; after all, the corresponding groups are not equal, but still mutually conjugate, so that they are in particular not normal subgroups of G.

Determining the fixed field of the remaining subgroups is more complicated, and you should definitely skip the rest of this case on a first reading.

Let us first consider the element $g_2 = (1\ 2)(3\ 4)$. We use a symmetrization trick, which we shall again encounter in Section VII.1, to find an element γ that generates the corresponding fixed field $M = L^{H_2}$. In fact, we will construct an element γ in M whose orbit under the action of the Galois group has cardinality 4. Then on the one hand we have $\mathbb{Q}(\gamma) \subset M$, but on the other hand Corollary III.2.5 implies that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. Since we know that

$$[M : \mathbb{Q}] \overset{1.2(\text{iii})}{=} [G : H_2] = \#(G/H_2) = \#G/\#H_2 = 8/2 = 4 \tag{34}$$

by Theorem 1.2(iii), we see that $M = \mathbb{Q}(\gamma)$ by the tower law. So having such an element γ at our disposal would be pretty swell.

Motivated by we know now what (for now), we take

$$\gamma = \beta_1^{-1}\beta_3^2 + \beta_2^{-1}\beta_4^2 \in L. \tag{35}$$

Then in fact $\gamma \in M$, since as G acts by permuting the indices, we see that the element $g_2 = (1\ 2)(3\ 4)$ satisfies

$$g_2(\gamma) = \beta_2^{-1}\beta_4^2 + \beta_1^{-1}\beta_3^2 = \gamma. \tag{36}$$

If we apply other non-trivial elements of G to γ, this never leads to an obvious equality $g_2(\gamma) = \gamma$ in the same way as in (36). It therefore stands to reason that the stabilizer of γ under G is generated by g_2. However, this argument is not a proof, as there may be hidden dependencies among the β_i.

Instead we repeatedly apply the element $r = (1\ 2\ 3\ 4)$ of G and compute the elements

$$\begin{aligned} \gamma &= \beta_1^{-1}\beta_3^2 + \beta_2^{-1}\beta_4^2 \\ &= \beta^{-1}(-\beta)^2 + (i\beta)^{-1}(-i\beta)^2 \\ &= (-1)^2\beta + i^{-1}(-i)^2\beta = (1+i)\beta, \end{aligned} \tag{37}$$

as well as

$$\begin{aligned} r(\gamma) &= \beta_2^{-1}\beta_4^2 + \beta_3^{-1}\beta_1^2 \\ &= (i\beta)^{-1}(-i\beta)^2 + (-\beta)^{-1}\beta^2 \\ &= i^{-1}(-i)^2\beta + (-1)\beta = (-1+i)\beta, \end{aligned} \tag{38}$$

and

$$\begin{aligned} r^2(\gamma) &= \beta_3^{-1}\beta_1^2 + \beta_4^{-1}\beta_2^2 \\ &= (-\beta)^{-1}\beta^2 + (-i\beta)^{-1}(i\beta)^2 \\ &= (-1)^{-1}\beta + (-i)^{-1}i^2\beta = (-1-i)\beta, \end{aligned} \tag{39}$$

and finally

$$\begin{aligned} r^3(\gamma) &= \beta_4^{-1}\beta_2^2 + \beta_1^{-1}\beta_3^2 \\ &= (-i\beta)^{-1}(i\beta)^2 + \beta^{-1}(-\beta)^2 \\ &= (-i)^{-1}i^2\beta + (-1)^2\beta = (1-i)\beta. \end{aligned} \tag{40}$$

Since $\#\{\gamma, r(\gamma), r^2(\gamma), r^3(\gamma)\} = 4$, we obtain that the Galois orbit of γ indeed has the desired length 4, so that $M = \mathbb{Q}(\gamma)$. Since $\gamma^4 = (1+i)^4\beta^4 = -4 \cdot 2$,

we conclude that the minimal polynomial of γ over $\mathbb{Q}$, which we know now to be quartic, is in fact given by $f = x^4 + 8 \in \mathbb{Q}[x]$.

As for the remaining subgroup $H_2' = \langle g_2' \rangle$, this is conjugate in D_4 to the previous subgroup H_2, as we have

$$g_2' = r^2 s = rsr^{-1} = rg_2 r^{-1}. \tag{41}$$

Using Exercise 5(i), we conclude that $M' = L^{H_2'}$ is another homomorphism of $M = \mathbb{Q}((1+i)\beta) \simeq \mathbb{Q}[x]/(x^4+8)$ into L. Moreover, (16) shows that

$$M' = r(M) = r(\mathbb{Q}(\gamma)) = (r\mathbb{Q})(r(\gamma)) = \mathbb{Q}(r(\gamma)) = \mathbb{Q}((-1+i)\beta). \tag{42}$$

Once again, neither of the fields

$$L^{H_2} = \mathbb{Q}((1+i)\sqrt[4]{2}) \quad \text{and} \quad L^{H_2'} = \mathbb{Q}((-1+i)\sqrt[4]{2}) = \mathbb{Q}((1-i)\sqrt[4]{2}) \tag{43}$$

is Galois over $\mathbb{Q}$; as the corresponding subgroups are mutually conjugate, they are not normal subgroups of G. In fact the proof of Theorem 2.3 implies that these two fields are two distinct images of homomorphisms of the abstract field extension $\mathbb{Q}[x]/(x^4+8)$ into L.

– $\mathbf{H^+ = \langle r^2 \rangle, \#(H/H^+) = 1}$: In this case $H = H^+ = \langle r^2 \rangle$, which is a normal subgroup of G. Now under $r^2 = (1\ 3)(2\ 4)$, the element $\beta^2 = \beta_1^2$ is sent to $\beta_3^2 = (-\beta_1)^2 = \beta_1^2 = \beta^2$. We conclude that $\beta^2 = \sqrt{2}$ is in the fixed field L^H. The same is the case for $i = (i\beta)/\beta = \beta_2/\beta_1$, since

$$r^2(\beta_2/\beta_1) = r^2(\beta_2)/r^2(\beta_1) = \beta_4/\beta_3 = (-i\beta)/\beta = i. \tag{44}$$

Therefore L^H contains the field $\mathbb{Q}(\sqrt{2}, i)$. As the two extensions in the chain

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(\sqrt{2}, i) \tag{45}$$

are of degree 2, we see that

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4 = [L^H : \mathbb{Q}] \tag{46}$$

by the tower law and Theorem 1.2(iii). We therefore conclude that

$$L^H = \mathbb{Q}(\sqrt{2}, i). \tag{47}$$

Since H is a normal subgroup of G, Theorem 2.3 shows that L^H is a Galois extension of $\mathbb{Q}$, which also follows directly from the fact that it is the splitting field of the separable polynomial $(x^2-2)(x^2+1) \in \mathbb{Q}[x]$. Its Galois group is isomorphic to $G/H \simeq V_4$, as can also be seen by the argumentation in Part (ii) of this above.

– $\mathbf{H^+ = \langle r^2 \rangle, \#(H/H^+) = 2}$: In this case H is one of the groups

$$H_1 = \langle r^2, s \rangle, \quad H_2 = \langle r^2, rs \rangle \tag{48}$$

both of which are isomorphic to the Vierergruppe V_4. Indeed, since $N = \langle r^2 \rangle$ is a normal subgroup of G, one of the corollaries of Noether's

isomorphism theorem shows that H is the inverse image of a subgroup of G/N of order 2. Now G/N is a group of order $\#(G/N) = \#G/\#N = 8/2 = 4$, and all its non-trivial elements $\overline{r}, \overline{s}, \overline{rs}$ have order dividing 2. The inverse image of $\overline{r}$ in G equals $H = \langle r^4 \rangle$, which cannot occur since then also $H^+ = \langle r^4 \rangle$, and we are left with the two other groups, whose inverse images in G are the groups H_1 and H_2 in (48).

Since all subgroups of the abelian group $G/N \simeq V_4$ are normal, the same is true for their inverse images in G, so that H_1 and H_2 are in fact normal subgroups of G. Alternatively, this follows from the fact that these subgroups have index $[G : H_i] = \#(G/H_i) = \#G/\#H_i = 8/4 = 2$ in G. For both these groups we have $\mathrm{Gal}(L^{H_i} \,|\, K) \simeq G/H_i \simeq C_2$.

Theorem 1.2(iii) now shows that the fixed fields $M_1 = L^{H_1}$ and $M_2 = L^{H_2}$ of the index-2 subgroups H_1 and H_2 of G are quadratic extensions of the base field $K = \mathbb{Q}$. They are therefore Galois by Example III.1.7(i), a fact that equally well follows from Theorem 2.3 in light of the normality of the subgroups H_i.

It remains to determine generators of the extensions M_1 and M_2. To this end, it suffices to find elements $\gamma_i \in M_i \setminus \mathbb{Q}$ by the argumentation in Example III.1.7(i). Let us first consider $\gamma_1 = \sqrt{-2} = i\sqrt{2} = (i\beta)\beta = \beta_1\beta_2$. Then since $r^2 = (1\ 3)(2\ 4)$ and $s = (1\ 2)(3\ 4)$ we see that

$$\begin{aligned} r^2(\beta_1\beta_2) &= \beta_3\beta_4 = (-\beta)(-i\beta) = i\beta^2 = \beta_1\beta_2 \quad \text{and} \\ s(\beta_1\beta_2) &= \beta_2\beta_1 = \beta_1\beta_2, \end{aligned} \tag{49}$$

so that indeed $\beta_1\beta_2 = \sqrt{-2} \in M_1 \setminus \mathbb{Q}$ and therefore

$$M_1 = L^{H_1} = \mathbb{Q}(\sqrt{-2}). \tag{50}$$

Now let us consider $\gamma_2 = \sqrt{2} = \beta^2 = \beta_1^2$. Then since $r^2 = (1\ 3)(2\ 4)$ and $rs = (1\ 3)$ we see that

$$\begin{aligned} r^2(\beta_1^2) &= \beta_3^2 = (\beta_1)^2 = \beta_1^2 \quad \text{and} \\ s(\beta_1^2) &= \beta_3^2 = (-\beta_1)^2 = \beta_1^2, \end{aligned} \tag{51}$$

so that indeed $\beta_1^2 = \sqrt{2} \in M_1 \setminus \mathbb{Q}$ and therefore

$$M_2 = L^{H_2} = \mathbb{Q}(\sqrt{2}). \tag{52}$$

– $\mathbf{H^+ = \langle r \rangle, \#(H/H^+) = 1}$: In this case $H = H^+ = \langle r \rangle$ is cyclic of order 4. This case can be dealt with in a similarly way to the previous one, finding a suitable generator by means of the permutation action. Alternatively, one notes that L^H is the sole remaining quadratic subextension of $L \,|\, K$ by Theorem 1.2, since H is the final subgroup of G of index 2 in our list.

Now $\mathbb{Q}(i) \,|\, \mathbb{Q}$ is a quadratic subextension of $L \,|\, \mathbb{Q}$ since $i \in L$. It cannot equal the real field $\mathbb{Q}(\sqrt{2})$, but it cannot equal the imaginary quadratic field $\mathbb{Q}(\sqrt{-2})$ either. After all if it did, the field $\mathbb{Q}(\sqrt{-2})$ would contain

the element $i\sqrt{-2} = \sqrt{2}$. We would get an inclusion $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{-2})$ and therefore an equality by the tower law since both fields are quadratic over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{R}$ and $\mathbb{Q}(\sqrt{-2})$ is not, this is absurd.

We can therefore conclude that the subextension $\mathbb{Q}(i)|\mathbb{Q}$ of $L|\mathbb{Q}$ does not equal either of the quadratic subextensions $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-2})|\mathbb{Q}$ that we already found. We conclude that

$$L^H = \mathbb{Q}(i) \tag{53}$$

for the subgroup $H = \langle r \rangle$ under consideration. As in the previous case we have $\mathrm{Gal}(L^H|K) \simeq G/H \simeq C_2$.

– $\mathbf{H^+ = \langle r \rangle, \#(H/H^+) = 2}$: In this case $H = D_4$ and

$$L^H = K = \mathbb{Q} \tag{54}$$

by Theorem III.2.3(ii). The Galois group is trivial. ❀

3 Extending the base field

Suppose that we know the Galois group of a polynomial $f \in K[x]$. One would suspect that this also allows us to say something about f considered as a polynomial in $M[x]$ for field extensions M of K. After all, if we denote the splitting field of f over K by L, then we have seen in Remark III.4.2(ii) that we can interpret the Galois group $\mathrm{Gal}(L|K)$ as the permutations of the zeros of f that extend to K-linear automorphisms of the splitting field L. If we instead consider f as a polynomial over the larger field M, then it is reasonable to surmise that the condition extending to an M-linear map is in general a more stringent one, so that the Galois group of f over can be identified with a subgroup of $\mathrm{Gal}(L|K)$.

This suspicion is true, but we need to set up the exact statement more conceptually. The main reason for this was alluded to in Remark I.1.14; whereas the motivation in the previous paragraph refers to a certain distinguished polynomial $f \in K[x]$ whose splitting field equals L, we would like our statements to be independent of such a choice. Another issue is that we have to specify in what "ambient" we combine the fields L and M. To this end, we at first simply suppose that there exists some finite Galois extension $K'|K$ that contains both L and M as subextensions. In fact the ideas underlying Exercise I.12 guarantees the existence of such an extension of K provided that L and M both be finite and separable. We now need an important definition that we also encountered in Exercise I.13.

Definition 3.1. Let $L|K$ and $M|K$ be subextensions of a larger extension $K'|K$. We define the COMPOSITUM LM of L and M to be the smallest subextension

$$LM := K\langle L, M \rangle \tag{55}$$

of $K'|K$ that contains both L and M. ✌

Example 3.2. In the situation of Definition 3.1, suppose that L is the splitting field of a polynomial $f \in K[x]$. Then we have

$$L = K(\beta_1, \dots, \beta_n), \tag{56}$$

where $\beta_1, \dots, \beta_n$ are the zeros of f considered as a polynomial in $K'[x]$, so that

$$f = (x - \beta_1) \cdots (x - \beta_n) \in K'[x]. \tag{57}$$

In this case the smallest field LM that contains both L and M is the subfield of K' that is generated by M and the zeros β_i. In other words, we have

$$LM = M(\beta_1, \dots, \beta_n). \tag{58}$$

We see that the extension $LM|M$ is once again a splitting field over M; in fact, it is the splitting field of f considered as a polynomial over the larger field M. ❀

Example 3.2 shows that the compositum is exactly the abstract notion that we need for the considerations at the start of this section. It will also allow us to make the upcoming main result somewhat more concrete.

Theorem 3.3. *Let $L|K$ and $M|K$ be subextensions of a finite Galois extension $K'|K$, and suppose that $L|K$ is normal. Let N and H be the subgroups of $G = \mathrm{Gal}(K'|K)$ that correspond to L and M, respectively. Then the following statements hold.*

(i) The subgroup of G that corresponds to the compositum LM is given by $H \cap N$.

(ii) The subgroup of G that corresponds to the intersection $L \cap M$ is given by

$$\langle H, N \rangle = HN := \{hn \,:\, h \in H, n \in N\}. \tag{59}$$

(iii) The extensions $LM \,|\, M$ and $L \,|\, L \cap M$ are Galois, and there is a canonical isomorphism

$$\begin{aligned} \mathrm{Gal}(LM|M) &\to \mathrm{Gal}(L|L \cap M) \\ \sigma &\mapsto \sigma|_L. \end{aligned} \tag{60}$$

Proof. (i): By definition, the compositum is the smallest subextension of the ambient extension $K'|K$ that contains both L and M. Theorem 1.2(ii) shows that under the Galois correspondence, this subextension corresponds to the largest subgroup of G that is contained in both H and N. This subgroup is nothing but the intersection $H \cap N$.

(ii): Reasoning as in Part (i), we see that this time we have to determine the smallest subgroup of G that contains both H and N. By definition, this subgroup is the subgroup $\langle H, N \rangle$ generated by H and N. It therefore remains to show that $\langle H, N \rangle = HN$.

Now certainly all the products hn in HN do belong to $\langle H, N \rangle$, so that $HN \subset \langle H, N \rangle$. Conversely, if we let $\pi : G \to G/N$ be the canonical quotient homomorphism, then

$$HN = \bigcup \{hN : h \in H\} = \bigcup_{h \in H} \pi^{-1}(hN) = \bigcup_{h \in H} \pi^{-1}(\pi(h)) = \pi^{-1}(\pi(H)), \tag{61}$$

and since the images and preimages of groups under group homomorphisms as again groups, we see that HN is a subgroup of G. By taking h (respectively n) equal to e in (60), we see that HN contains N (respectively H). Since $\langle H, N\rangle$ is by definition the smallest subgroup of G that contains both H and N, we obtain the converse inclusion $\langle H, N\rangle \subset HN$, and with that we are done.

(iii): Since $L|K$ is finite normal, Example 3.2 shows that the same is true for the extension $LM|M$. This extension is also separable; since $K'|K$ is Galois, all elements of K' are separable over K, and therefore a fortiori over M. Therefore $LM|M$ is in fact finite Galois. Moreover, since $L \cap M$ contains K, the extension $L|L \cap M$ is also Galois in light of Proposition 2.1; after all, the finite normal extension $L|K$ is Galois in light of Theorem 2.3.

Let us consider the restriction map

$$\begin{aligned} \mathrm{Gal}(LM|M) &\to \mathrm{Gal}(L|K) \\ \sigma &\mapsto \sigma|_L. \end{aligned} \tag{62}$$

First, the map (62) is well-defined; because L is a normal extension of K, it is mapped into itself by any $\sigma \in \mathrm{Gal}(LM|M)$ in light of Theorem 1.10(ii) (applied to $\varphi = \mathrm{id}$ and $\varphi' = \sigma$). Second, since

$$(\sigma \circ \sigma')|_L = \sigma_L \circ \sigma'_L, \tag{63}$$

we conclude that (62) is in fact a homomorphism. Third, the map (62) is injective. Indeed, let $\sigma \in \mathrm{Gal}(LM|M)$ be an element of its kernel. Then σ fixes the subfield M by definition. If σ moreover restricts to the identity element of $\mathrm{Gal}(L|K)$, then σ fixes L as well. Since the set of elements of LM that are fixed by σ is a subfield of M by Exercise III.4, we see that σ must fix the compositum LM as well, since after all this is by definition the smallest subextension of $K'|K$ that contains both L and M. This implies that σ is in fact the identity automorphism of $LM|M$, and since σ was arbitrary, we obtain the claimed injectivity.

It remains to determine the image of (62). To this end, consider an element $\beta \in L$. Then applying Theorem III.2.3(ii) to the Galois extension $LM|M$, we obtain that β is fixed under the image of (62) if and only if β belongs to M, which is the case if and only if $\beta \in L \cap M$ since we assumed β to be an element of L. Expressed differently, we have shown that the fixed field of the image of (62) is $L \cap M$. The bijective correspondence from Theorem 1.2(i) then implies that said image equals $\mathrm{Gal}(L|L \cap M)$, and with that, the proof of the theorem is concluded. ♡

Remark 3.4. (i) If L is the splitting field of a separable polynomial $f \in K[x]$, then Example 3.2 shows that $\mathrm{Gal}(LM|M)$ is the Galois group of f considered as a polynomial over M. This equation then gives a way to identify this Galois group with the subgroup $\mathrm{Gal}(L|L \cap M)$ of the original Galois group $\mathrm{Gal}(L|K)$, which was our hope at the start of this section. See Example 3.5 below for some concrete considerations.

(ii) Let us spend a few more lines on what exactly is going on in the proof of Part (ii) of Theorem 3.3. In fact, it is essential that N be a normal subgroup

of G for HN again to be a subgroup, as we can then rewrite any product $h_1n_1h_2n_2$ of its elements as

$$h_1n_1h_2n_2 = h_1en_1h_2n_2 = h_1h_2h_2^{-1}n_1h_2n_2 = (h_1h_2)((h_2^{-1}n_1h_2)n_2), \tag{64}$$

which belongs to HN since $h_2^{-1}n_1h_2 \in N$ by normality of N in G. In this way, we can reduce any element

$$h_1n_1 \cdots h_rn_r \in \langle H, N\rangle \tag{65}$$

to the form $hn \in HN$. Similarly, we can rewrite the inverse $(hn)^{-1}$ of an element of HN as

$$(hn)^{-1} = n^{-1}h^{-1} = en^{-1}h^{-1} = h^{-1}hn^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}), \tag{66}$$

which belongs to HN since $hn^{-1}h^{-1} \in N$ by normality of N in G. If N is not normal in G, then in general HN will not be a subgroup of G, and there will only exist an inclusion $HN \subset \langle H, N\rangle$. ❁

Example 3.5. Let us consider the splitting field L of the polynomial $f = x^4 - 2$ from Example 2.7 as the subfield $\mathbb{Q}(\sqrt[4]{2}, i)$ of $\mathbb{C}$, and let $M \subset \mathbb{C}$ be another subfield. Theorem 3.3 shows that the Galois group $H = \mathrm{Gal}(LM \,|\, M)$ of the splitting field of f depends only on what the intersection $L \cap M$ is, and H can be determined with the aid of the calculations in said example, namely as follows.

(i) If $L \cap M = \mathbb{Q}$, then $H \simeq D_4$.

(ii) If $L \cap M = \mathbb{Q}(i)$, then $H \simeq C_4$.

(iii) If $L \cap M$ equals $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$, then $H \simeq V_4$.

(iv) If $L \cap M$ equals $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}((1+i)\sqrt[4]{2})$, or $Q((1-i)\sqrt[4]{2})$, then $H \simeq C_2$.

(v) If $L \cap M$ equals $\mathbb{Q}(\sqrt[4]{2}, i) = L$ then H is trivial. ❀

Here is a useful corollary of Theorem 3.3. For a more abstract similar result, see Exercise 8.

Corollary 3.6. *Let $L|K$ be a subextension of a larger ambient extension $K'|K$, and let $\gamma \in K'$ be algebraic. Let f (respectively g) be the minimal polynomial of γ over K (respectively over L). If $L|K$ is a finite Galois extension, then the following statements are equivalent.*

(i) $f = g$.

(ii) $[K(\gamma) : K] = [L(\gamma) : L]$.

(iii) $L \cap K(\gamma) = K$.

Proof. (i) $\Leftrightarrow$ (ii): Since f is a polynomial in $L[x]$ such that $f(\beta) = 0$ and g is the minimal polynomial of β over L, we know that g divides f. Since the theory of simple extensions shows that $\deg(f) = [K(\beta) : K]$ and $\deg(g) = [L(\beta) : L]$, we have $[K(\beta) : K] = [L(\beta) : L]$ if and only if $\deg(f) = \deg(g)$. Since f and g are both monic, this in turn is equivalent to the equality $f = g$.

(ii) $\Leftrightarrow$ (iii): Consider the finite subextension $K(\gamma)|K$ of $K'|K$. Then we have

$$[L(\gamma) : L][L : K] = [L(\gamma) : K] = [L(\gamma) : K(\gamma)][K(\gamma) : K]. \tag{67}$$

Therefore (ii) holds if and only if $[L : K] = [L(\gamma) : K(\gamma)]$. Now applying Theorem 3.3 to the finite extension $M = K(\gamma)$, we obtain

$$\begin{aligned}[L(\gamma) : K(\gamma)] = [LM : M] &= \#\mathrm{Gal}(LM|M) = \#\mathrm{Gal}(L|L \cap M) \\ &= \#\mathrm{Gal}(L|L \cap K(\gamma)).\end{aligned} \tag{68}$$

We also have

$$[L : K] = \#\mathrm{Gal}(L|K). \tag{69}$$

Therefore $[L(\gamma) : K(\gamma)] = [L : K]$ if and only if $\#\mathrm{Gal}(L|L \cap K(\gamma)) = \#\mathrm{Gal}(L|K)$. Since $\mathrm{Gal}(L|L \cap K(\gamma))$ is a subgroup of the finite group $\mathrm{Gal}(L|K)$, this equality holds if and only if $\mathrm{Gal}(L \mid L \cap K(\gamma)) = \mathrm{Gal}(L \mid K)$, and the bijectivity of the correspondence in Theorem 1.2(i) implies that this is the case if and only if $L \cap K(\gamma) = K$. ♡

Remark 3.7. (i) Note that Part (iii) of Theorem 3.3 does not actually refer to the ambient extension $K'|K$, and indeed, Example 3.2 shows that if L is the splitting field of a polynomial $f \in K[x]$, then we can equally well realize the compositum LM as the splitting field of the polynomial f over M, thus obviating any need for the larger extension $K'|K$. There are two reasons why the ambient was still mentioned in Theorem 3.3. The first is our insistence on the relation of Galois theory with group theory, which did play a role in Parts (i) and (ii) of Theorem 3.3. In fact, Part (iii) of the theorem also admits an extremely charming proof using group theory; in this language, it translates into the canonical isomorphism

$$\begin{aligned}H/(H \cap N) &\xrightarrow{\sim} HN/N \\ h(H \cap N) &\mapsto hN,\end{aligned} \tag{70}$$

which is one of the consequences of Noether's isomorphism theorem; see Exercise 10. Thus group theory reflects field theory once again.

(ii) The second and far more serious reason to refer to an ambient occurs in the case where neither of the extensions $L|K$ and $M|K$ is Galois. Indeed, whereas the image of L inside K' is uniquely determined by Theorem I.1.10 when $L|K$ is Galois, the same cannot be said in general. For example, let us take both L and M to equal the abstract extension $\mathbb{Q}[x]/(x^3 - 2)$ of $\mathbb{Q}$. If we embed L into $\mathbb{C}$ as $\mathbb{Q}(\sqrt[3]{2})$ and do the same for M, then $LM = \mathbb{Q}(\sqrt[3]{2})$. However, if we realize M as the subfield $\mathbb{Q}(\zeta\sqrt[3]{2})$ of $\mathbb{C}$ instead, then we obtain

$$LM = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}) = \mathbb{Q}(\zeta_3, \sqrt[3]{2}), \tag{71}$$

which is a sextic number field that is not even of the same degree as the previous cubic compositum $\mathbb{Q}(\sqrt[3]{2})$. We see that if neither $L|K$ nor $M|K$ is normal, the compositum all of a sudden becomes ill-defined even up to K-isomorphism in the absence of a specific choice of K-homomorphisms of L and M into a larger extension K'.

This is not an overly precise abstract gripe; most of the results in this section simply collapse if neither $L|K$ nor $M|K$ is Galois. Not only does Theorem 3.3 no longer apply, but Corollary 3.6 ceases to be true as well.

For example, consider the statement of Corollary 3.6 for the finite non-Galois subextension $L = \mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ of $\mathbb{C}|\mathbb{Q}$ and $\gamma = \zeta_3\sqrt[3]{2}$. Since $\gamma \notin L$, the intersection $L \cap \mathbb{Q}(\gamma)$ is the unique proper subfield $\mathbb{Q}$ of $\mathbb{Q}(\gamma)$. Therefore the condition in Corollary 3.6(iii) is satisfied. However, neither of the other conditions is satisfied; since $L(\gamma) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})$ is the splitting field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ of f over $\mathbb{Q}$, it is in fact of degree 6 over $\mathbb{Q}$ by Example III.1.7(ii) and therefore of degree 2 over $\mathbb{Q}(\sqrt[3]{2})$ by the tower law, whereas Corollary 3.6(i) would imply that this degree equals 3.

Similarly, we see that Corollary 3.6(ii) does not hold, since Example I.1.3(ii) shows that the minimal polynomial of $\zeta_3\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt[3]{2})$ is of degree $2 \neq 3$. For more general version of such unpleasant behavior, see Exercise 8(ii).

Whatever point of view one prefers, the gist of this remark is that composita have ill-defined behavior for non-Galois extensions that do not come with an embedding into a larger ambient. The right way to deal with such abstract extensions requires us to enlarge our world to include TENSOR PRODUCTS and ÉTALE ALGEBRAS, but these topic are beyond the scope of these notes. However, see [Mil22, Chapter 8] for a sketch of this more complete theory.

(iii) It is also possible to study the Galois group upon restriction of the base field K, or equivalently for a tower of Galois extensions $K \subset L \subset M$; however, this is another topic that we shall not engage with. Suffice to say that even starting on it is complicated enough; though both quadratic extensions in the chain $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$, the same is not true for their composition $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$. See Exercise 9 for what can happen in the simplest case of successive quadratic extensions. ❁

4 The primitive element theorem*

While Galois theory is not strictly needed to prove the following theorem in this optional section, it does make the proof a tad more insightful. After it, we briefly discuss some other fruitful viewpoints on field theory that are provided by Galois' results.

Theorem 4.1 (Primitive element theorem)**.** *Let $L|K$ be a finite separable field extension. Then there exists an element $\beta \in L$ such that $L = K(\beta)$.*

Proof. If the field K is finite, then the same is true for its finite extension L. Now the theory of finite fields shows that L^* is a cyclic group, and if β is a generator

of L^*, then the subfield $K(\beta)$ of L contains both 0 and all of L^*, so that in fact $K(\beta) = L$. We may therefore assume that the field K is infinite, and certainly we may also assume that $[L : K] > 1$, since otherwise $L = K(0)$.

Since $L \mid K$ is finite, we can find $\beta_1, \ldots, \beta_n$ in L such that $L = K(\beta_1, \ldots, \beta_n)$. Since $L \mid K$ is separable, the same is the case for the minimal polynomials f_i of the elements β_i. We may rearrange the polynomials f_i in such a way that the first $r \leq n$ among them are mutually distinct and such that the remaining polynomials $f_{r+1}, \ldots, f_n$ among them (if any) coincide with one of the preceding polynomials $f_1, \ldots, f_r$. Since the f_i are all monic and irreducible, the mutual greatest common divisors of the polynomials $f_1, \ldots, f_r$ equal 1; therefore their least common multiple f is simply the product $f_1 \cdots f_r$. By our assumptions on $f_{r+1}, \ldots, f_n$, this least common multiple f is in fact divisible by all polynomials $f_1, \ldots, f_n$, and therefore by their least common multiple as well.

We claim that f is separable. To this end, let γ be a zero of f. Then γ is a zero of one of the polynomials $f_1, \ldots, f_r$, say of f_i. Since f_i is monic and irreducible, it must be the minimal polynomial of γ. Now γ cannot be a zero of any other polynomial f_j, since then we could once more conclude that f_j is the minimal polynomial of γ, a contradiction with the fact that the polynomials $f_1, \ldots, f_r$ are distinct. We see that the multiplicity of γ as a zero of f_i equals 1, whereas its multiplicity as a zero of f_j with $j \neq i$ equals 0. Therefore γ is also of multiplicity 1 as a zero of f. Since γ was arbitrary, this shows that f is indeed separable.

Let N be the splitting field of f over K. The prolongation lemma 1.4 implies that there exists a K-homomorphism $L \to N$. Now the field extension $L \mid K$ is finite Galois by Proposition III.1.5, and its Galois group $G = \mathrm{Aut}(N \mid K)$ is of finite cardinality $[N : K]$. In particular, this finitude implies that G has at most finitely many subgroups. Theorem 1.2(i) therefore shows that N has only finitely many proper subextensions. A fortiori, the field extension $L|K$ itself has only finitely many proper subextensions, say $M_1 \mid K, \ldots, M_s \mid K$.

We now consider L as a K-vector space of finite dimension $d = [L : K] > 1$. As the proper subextensions $M_1, \ldots, M_s$ of $L|K$ are also proper K-subvector spaces of L, we can find hyperplanes $H_1, \ldots, H_s$ of dimension $d - 1$ that contain them. If we can show that there exists an element β of L that does not belong to any of these hyperplanes H_i, then certainly the subextension $K(\beta) \mid K$ cannot be contained in any of the proper subextensions $M_i \mid K$, so that perforce $K(\beta) = L$.

It remains to show that we can find such an element β. To this end, we choose a K-basis of L, so that we can consider L as the standard vector space K^d. In this way, the hyperplanes $H_1, \ldots, H_s$ admit defining equations

$$H_i : \alpha_{i,1} x_1 + \ldots + \alpha_{i,d} x_d = 0 \tag{72}$$

with $\alpha_{i,j} \in K$ for $1 \leq j \leq d$. We prove the existence of an element $\beta \in K^d$ such that $\beta \notin H_i$ for $1 \leq i \leq s$ by induction on the dimension d.

If $d = 1$, then all H_i equal the zero subvector space, so that we can take β to equal any non-zero element of K^d. Now suppose that the statement is proved for $d - 1$. We can then find $\beta_1, \ldots, \beta_{d-1} \in K$ such that

$$\alpha_{i,1}\beta_1 + \ldots + \alpha_{i,d-1}\beta_{d-1} \neq 0 \tag{73}$$

for all $1 \leq i \leq s$ for which the hyperplane equation H_i from (72) remains non-trivial when removing the variable x_d. It remains to determine β_d such that

moreover

$$\alpha_{i,1}\beta_1 + \ldots + \alpha_{i,d-1}\beta_{d-1} + \alpha_{i,d}\beta_d \neq 0 \tag{74}$$

for all $1 \leq i \leq s$. Let us take $\beta_1, \ldots, \beta_{d-1} \in K$ as in (73). If we take $\beta_d \neq 0$, then certainly (73) is satisfied for all i such that H_i is defined by the equation $x_d = 0$. For all other i, the equation (74) is satisfied provided that

$$\beta_d \neq -\alpha_{i,d}^{-1}(\alpha_{i,1}\beta_1 + \ldots + \alpha_{i,d-1}\beta_{d-1}). \tag{75}$$

Since K is infinite, we can indeed find a non-zero $\beta_d \in K$ such that (75) is satisfied for $1 \leq i \leq s$. Taking $\beta = (\beta_1, \ldots, \beta_d)$, we obtain the requested element $\beta \in K^d$ outside the hyperplanes $H_1, \ldots, H_s$, which proves our claim, and with it the theorem. ♡

Remark 4.2. (i) The hypothesis that $L|K$ be separable in Theorem 4.1 cannot be omitted, as there exist finite inseparable field extensions that are not simple, such as that in Example II.2.13(ii). Similarly, while the proof of Theorem 4.1 shows that any finite separable field extension only has finitely many proper subfields, the same is not true when the separability condition is omitted; see Exercise 2.

(ii) The field N constructed in the proof of Theorem 4.1 is nothing but the normal closure from Exercise I.12.

(iii) Theorem 4.1 implies that every finite Galois extension $L|K$ is the splitting field of a separable irreducible polynomial $f \in K[x]$; also see Exercise III.1. Indeed, let $\beta \in L$ is such that $L = K(\beta)$, and let f be the minimal polynomial of β over K. Then L contains all zeros of f, since it is a normal extension of K. Therefore L also contains the splitting field of f over K. However, since L is generated by a zero of f, it is also contained in the splitting field of f, so that it in fact coincides with this field. ❁

In a sense, the proof of Theorem 4.1 shows that if the base field K is infinite, almost every element β of the finite separable extension L has the property that $K(\beta) = L$. In fact, the exceptional β are contained in a union of hyperplanes that can be determined explicitly once $\mathrm{Aut}(N|K)$ is known. It is in fact often useful to describe a field extension L as a vector spaces over its base field K; in this way, the subextensions of $L|K$ are simply special K-subvector spaces of L and the automorphisms $\sigma \in \mathrm{Aut}(L|K)$ are K-linear isomorphisms from L to itself. This is useful in many ways; for example, determining the fixed field of a given subgroup $H \subset \mathrm{Aut}(L|K)$ reduces to determining the intersections of the kernels of generators of H. This linear-algebraic point of view can also be used to explicitly describe field extensions in terms of radical by means of Section VII.3 (and particularly its Exercise 23) will show.

5 Exercises for Chapter IV

Exercise 1. Let $M|K$ be a subextension of a Galois extension $L|K$. Show that the subset $\mathrm{Aut}(L|M)$ of $\mathrm{Aut}(L|K)$ defined in (4) is indeed a subgroup of $\mathrm{Aut}(L|K)$.

Exercise 2. Let p be a prime, let F be a field of characteristic p, let K be the rational function field $K = F(t,u)$, and let

$$L = K(\beta,\gamma) = F(t^{1/p}, u^{1/p})$$

be the field extension from Example II.2.13(ii). Show that the field extension $L|K$ has infinitely many subextensions.

Exercise 3. Let $f \in K[x]$ be a separable polynomial of degree n, and let G be its Galois group, considered as a subgroup of S_n by means of some numbering of the zeros β_i of f in $\overline{K}$, and therefore acting on the set $\{1,\dots,n\}$.

(i) Show that $K(\beta_i)|K$ is the fixed field of the stabilizer $S^G(i)$ of i in G.

(ii) Show that if f is irreducible, then all fields $K(\beta_i)|K$ are isomorphic to the stem field of f.

Exercise 4. Let $M|K$ be a subextension of a Galois extension $L|K$. Let $G = \mathrm{Gal}(L|K)$, and let H be the subgroup $\mathrm{Gal}(L|M)$ of G.

(i) Let

$$N = N_G(H) = \{\sigma \in G : \sigma H = H\sigma\}$$

be the NORMALIZER of H in G. Show that H is a normal subgroup of N.

(ii) Show that there is a canonical isomorphism

$$\begin{aligned} N/H &\xrightarrow{\sim} \mathrm{Aut}(M|K) \\ \sigma H &\mapsto \sigma|_M. \end{aligned}$$

Exercise 5. Let $M|K$ be a subextension of a Galois extension $L|K$. Let $G = \mathrm{Gal}(L|K)$, and let H be the subgroup $\mathrm{Gal}(L|M)$ of G. Let us define the normalizer $N = N_G(H)$ as in the previous exercise.

(i) Let H' be another subgroup of G. Use the prolongation lemma 1.4 to show that $L^{H'}$ is K-isomorphic to M if and only if H' is G-conjugate to H.

(ii) Show that the association

$$\sigma \rightsquigarrow \sigma(M) \subset L$$

induces a bijection between the coset space G/N and the set of subfields of L that are K-isomorphic to M.

(iii) Conclude that the number of distinct images of the K-homomorphisms of M into $\overline{K}$ equals $\#G/N$. In other, slightly less precise words: Show that M can be realized in exactly $\#G/N$ ways as a subfield of $\overline{K}$.

Exercise 6. Let $f \in K[x]$ be a separable irreducible polynomial of degree n, with stem field $L = K[x]/(f)$. Let G be the Galois group of f, considered as a subgroup of S_n by means of some numbering of the zeros of f in $\overline{K}$. Let $H \subset G$ be the stabilizer of 1, and let $N = N_G(H)$.

Show that the stem field L can be realized in exactly $\#G/N$ ways as a subfield of $\overline{K}$ (in the sense of Part (iv) of the previous exercise).

Exercise 7. Show that Corollary 3.6 also holds for arbitrary (not necessarily finite) Galois extensions $L|K$.

Exercise 8. Let $L|K$ and $M|K$ be finite subextensions of an ambient extension $LM|K$.

(i) Show that if $L|K$ is Galois, then

$$[LM : K] = \frac{[L : K][M : K]}{[L \cap M : K]}.$$

(ii) Show that Part (i) may not hold if neither $L \mid K$ nor $M \mid K$ is a Galois extension.

Exercise 9. Let K be a field of characteristic not equal to 2, let $L|K$ be a quadratic extension of the form $L = K(\sqrt{\alpha})$, and let $M|L$ be a quadratic extension of the form $M = L(\sqrt{\beta})$. Let N be the normal closure of the extension $M|K$, in the sense of Exercise I.12. Finally, let σ be a generator of $\mathrm{Gal}(L|K)$.

(i) Show that if $\beta\sigma(\beta) \in (K^*)^2$, then $N = L$ and $\mathrm{Gal}(N|K) \simeq D_4$.

(ii) Show that if $\beta\sigma(\beta) \in \alpha(K^*)^2$, then $N = L$ and $\mathrm{Gal}(N|K) \simeq C_4$.

(iii) Show that if neither of the previous conditions is fulfilled, then N is a quadratic extension of M and $\mathrm{Gal}(N|K) \simeq D_4$.

Exercise 10. Let $L|K$ and $M|K$ and the corresponding subgroups N and H be as in Theorem 3.3(iii).

(i) Use Theorem 2.3 to obtain a canonical isomorphism $\mathrm{Gal}(LM|M) \simeq H/H \cap N$.

(ii) Use Theorem 2.3 to obtain a canonical isomorphism $\mathrm{Gal}(L \mid L \cap M) \simeq HN/N$.

(iii) Show that under the isomorphisms from Part (i) and (ii), the isomorphism in (60) translates to the homomorphism (70).

Exercise 11. Let $f \in K[x]$ be a polynomial of degree $n > 0$ with $\mathrm{Gal}(f) = S_n$. Show that the stem field $L|K$ only admits itself and the trivial extension $K|K$ as subextensions.

Exercise 12. Let $K|\mathbb{Q}$ be a number field. Given a homomorphism $\iota : K \to \mathbb{C}$, we define its complex conjugate $\bar{\iota} : K \to \mathbb{C}$ by $\bar{\iota}(\alpha) = \overline{\iota(\alpha)}$.

(i) Show that given a homomorphism $\iota : K \to \mathbb{C}$, there exists at most one $\rho \in \mathrm{Aut}(K)$ such that $\bar{\iota} = \iota\rho$.

(ii) Show that in general, the automorphism ρ from Part (i) may depend on the chosen homomorphism ι.

(iii) Suppose that if there exists an automorphism $\rho \in \mathrm{Aut}(K)$ such that $\bar{\iota} = \iota\rho$ for **all** homomorphisms $\iota : K \to \mathbb{C}$, then the fixed field K^ρ is TOTALLY REAL, in the sense that the image of any homomorphism $K^\rho \to \mathbb{C}$ is contained in $\mathbb{C}$.

(iv) In the situation of (iii), show that if $K^\rho \neq K$, then $K = K^\rho(\sqrt{w})$, where $w \in K^\rho$ is TOTALLY NEGATIVE, meaning that $\iota(w) \in \mathbb{R}_{<0}$ for all $\iota : K^\rho \to \mathbb{C}$.

(v) Conversely, show that if K is a quadratic extension $F(\sqrt{w})$ of a totally real field F with $\iota(w) \in \mathbb{R}_{<0}$ for all $\iota : F \to \mathbb{C}$, then K admits an automorphism ρ as in (iii).

The number fields described in Parts (iii)-(v) of this exercise are called CM FIELDS, where CM stands for COMPLEX MULTIPLICATION. The automorphism ρ is called the COMPLEX CONJUGATION of the CM field K.

Exercise 13. Let $K|\mathbb{Q}$ be a CM field, as defined in the previous exercise.

(i) Show that the normal closure $L|\mathbb{Q}$ of $K|\mathbb{Q}$, as defined in Exercise 9, is again a CM field.

(ii) Show that the complex conjugation of $L|\mathbb{Q}$ commutes with all elements of $\mathrm{Gal}(L|\mathbb{Q})$.

Exercise 14. For each of the following pairs K and f, determine all the subextensions of the splitting field of f. Moreover, determine which of these subextensions are normal over K, and compute the corresponding Galois groups.

(i) $K = \mathbb{Q}$, $f = x^3 - 5$.

(ii) $K = \mathbb{Q}(\sqrt{3})$, $f = x^3 - 5$.

(iii) $K = \mathbb{Q}(\sqrt{-3})$, $f = x^3 - 5$.

(iv) $K = \mathbb{F}_3$, $f = x^3 - x - 1$.

(v) $K = \mathbb{Q}$, $f = x^4 + 5$.

(vi) $K = \mathbb{Q}$, $f = x^4 + x^3 + x^2 + x + 1$.

(vii) $K = \mathbb{Q}$, $f = x^4 - x^2 + 1$.

Exercise 15. For devout non-believers: State and prove all the results in this chapter without making use of an algebraic closure.

Summary and main notions of the chapter

We answer Questions (i)-(iii) from the introduction to this chapter:

(i) Given a subgroup $H \subset G = \mathrm{Gal}(L|K)$, we associate to it the subextension $M|K$ of $L|K$ that is given by the fixed field $M = L^H$ from Definition III.2.1.

(ii) Given a subextension $M|K$ of $L|K$, we associate to it the subgroup $H \subset G$ of $G = \mathrm{Gal}(L|K)$ that is given by the fix group $\mathrm{Gal}(L|M)$ from Definition III.1.1.

(iii) Theorem 1.2(ii) shows that an inclusion $H \subset H'$ gives rise to an inclusion of fixed fields $L^{H'} \subset L^H$ in the other direction. Moreover, it shows that the degree $[L : L^H]$ equals $\#H$, whereas the degree $[L^H : K]$ equals the index $[G : H]$.

Theorem 2.3 shows that H is a normal subgroup of G if and only if the extension $L^H|K$ is Galois (the extension $L|^{H}$ is always Galois). Finally, Theorem 3.3 gives a complete group-theoretic description of the effect of the field-theoretic operation of extending the base field K.

The key skills to take away from this are the following:

– You are aware of the Galois correspondence in Theorem 1.2 and its properties, and you know how to make this explicit for examples of small degree such as quadratic fields (Example 1.3(i)), cubic fields (Example 1.3(ii) and (iii)), and quartic fields (Example 2.5(ii) and 2.7).

– You can characterize the Galois group of normal subextensions of a given finite Galois extensions as a quotient group, both in theory (Theorem 2.3) and in practice (Example 2.7).

– You can describe the behavior of the Galois group under extension of the base field, both in theory (Theorem 3.3) and in practice (Example 3.5).

– (Optional) You are aware of the constructive proof of the primitive element theorem 4.1 by means of Galois theory.

Chapter V

Computing Galois groups

It is in itself good to know that Galois groups of fields and polynomials exist, and that they have many fascinating and relevant applications. However, any mathematical theory that has practical consequences (that is, any such theory that is of any interest whatsoever) has to ask itself whether it can actually be worked with in practice. It would be highly disappointing if the theoretical results of Galois theory were only somewhere "out there" without any way to get at them computationally.

Though this is the longest chapter in these notes, its goal is quite modest, and it only has a single motivating question:

(i) Let $f \in K[x]$ be a separable irreducible polynomial of small degree, with splitting field L. Can we compute the Galois group $G = \mathrm{Gal}(f) = \mathrm{Gal}(L|K)$ in terms of simple data that can be effectively calculated once f is given?

This question is phrased somewhat vaguely. So let us spell out the fine print. In this chapter, "of small degree" means "of degree at most 4", which is certainly a completely arbitrary bound, but well, that is our bound and we stick with it. The project in Section VII.1 will push the methods of this chapter a bit further to degree 5, and also has some words to say about the general approach, called Stauduhar's algorithm, which becomes exponentially more complicated as the degree of f increases; but see Section VII.2 for alternative methods that often quickly determine the Galois group of f.

One of the main tools for determining the Galois group of a polynomial $f \in K[x]$ is provided by its various resolvents. These are polynomials $g \in K[x]$ that can be computed starting from f; if such a resolvent g is square-free and admits a simple zero in K, then this often implies that the Galois group of the original polynomial f is smaller than is generically the case. Taking multiple resolvent allows one to decrease the possibilities for G until only the correct answer is left.

The systematic study of resolvents, on which Stauduhar's algorithm is based, quickly becomes highly complicated, but in small degree, these resolvents are still pleasant enough. For polynomials of degree 3, we first meet them in the guise of the discriminant, and for polynomials of degree 4, the determination

of the Galois group hinges on the determination of the zeros in the ground field K (if any) of the associated RESOLVENT CUBIC. This leads to a classification of the Galois group that is still quite pleasant and friendly, in contrast to the far more elaborate situation in higher degree. Incidentally, resolvents were first developed in the context of the question on resolvability in terms of radicals that motivated Galois to develop his theory, as described in Section VII.3.

We conclude this introduction with a slightly vague yet worthwhile remark, namely that if K is a number field, then a "random" polynomial $f \in K[x]$ of degree n is irreducible with "full" Galois group S_n with probability 1. (The vagueness of this statement lies in the fact that we neglect to state the precise probability measure on $K[x]$.) An example of a family of polynomials in $\mathbb{Q}[x]$ with Galois group S_n is given by

$$f = x^n - x - 1 \in \mathbb{Q}[x]. \tag{1}$$

In Section VII.2, you will see some simple criteria to decide when an irreducible polynomial $f \in K[x]$ with coefficients in K has Galois group S_n. In fact, polynomials with this "generic" Galois group are in practice far easier to deal with than polynomials with smaller Galois groups, which require Stauduhar's subtle considerations on resolvents.

While polynomials over number fields usually have the full symmetric group as their Galois group, the converse is true for polynomials over finite fields $\mathbb{F}_q$. In fact, the Galois group of an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree n is always cyclic of order n, and it is generated by the FROBENIUS AUTOMORPHISM

$$\begin{aligned} \sigma_q : L &\to L \\ \beta &\to \beta^q. \end{aligned} \tag{2}$$

This especially elegant behavior is a consequence of the general theory of finite fields once this is reinterpreted in the context of Galois theory in Section 3. We conclude the chapter with brief discussions of cyclotomic fields (in Section 4) and the inverse Galois problem (in Section 5).

1 Methods for degree 3

In the upcoming sections, we will consider the Galois group of separable polynomials $f \in K[x]$ of small degree, and in this section we start with cubic polynomials; the case of quadratic polynomials was already fully considered in Example III.4.4(i). Moreover, we will throughout this chapter mostly restrict our attention to separable polynomials f that are moreover **irreducible**; as we saw in Example III.4.4(ii), in the absence of this assumption the case distinction gets fairly complicated already in the cubic case.

Given a separable irreducible polynomial f of general degree n, we will always choose some labeling of its zeros $\beta_1, \dots, \beta_n$ in its splitting field $L \mid K$. Theorem 4.1 shows that this allows us to interpret $G = \mathrm{Gal}(f) := \mathrm{Gal}(L \mid K)$ as a subgroup of S_n, and that the irreducibility of f translates into the property that G acts transitively on $\{1, \dots, n\}$. We should therefore first see what transitive subgroups of S_n exist, starting with the current case $n = 3$.

Proposition 1.1. *Let $G \subset S_3$ be a transitive subgroup. Then exactly one of the following possibilities holds.*

(i) $G = A_3$.

(ii) $G = S_3$.

Proof. Since G is transitive, the orbit of its action on the set $\{1,2,3\}$ has cardinality 3. The orbit-stabilizer theorem then implies that $3 \mid \#G$ is divisible by 3. By Cauchy's theorem, G contains an element σ of order 3, and such an element in S_3 is a 3-cycle. On the other hand, we have $\#G|\#S_3 = 3! = 6$. Therefore $\#G \in \{3,6\}$. If $\#G = 6$, then $G = S_3$. If $\#G = 3$, then $G = \langle\sigma\rangle$, since $\langle\sigma\rangle \subset G$ and both groups are of cardinality 3. Since any 3-cycle in S_3 generates A_3, we must then have $G = A_3$. ♡

In light of Example III.1.7(ii), Proposition 1.1 is not surprising: If Case (i) in the proposition applies, then $[L : K] = \#G = 3$ by Theorem III.1.2, so that the splitting field L coincides with the cubic stem field of f. By Corollary I.1.13, this occurs exactly when f splits over its stem field, which is Case (a2) in Example III.1.7(ii). In Case (ii), we have $[L : K] = \#G = 6$, so that the splitting field L of f is a proper extension of its stem field; this is Case (a1) in Example III.1.7(ii).

In a sense, we have completely solved the question under consideration. However, the answer is not satisfying, because we have neglected certain natural questions:

(i) Given $f \in K[x]$, can we effectively decide which of the cases in Proposition 1.1 applies?

(ii) Suppose that we are in Case (ii) of Proposition 1.1. Theorem IV.1.2 implies that K admits a quadratic extension inside the splitting field L, which corresponds to the subgroup $A_3 \subset S_3$. Can we describe this quadratic extension explicitly?

To solve this question, we need a classical notion, a special case of which you will already have encountered in high school.

Definition 1.2. Let $f \in K[x]$ be a polynomial of degree n such that

$$f = \alpha(x-\beta_1)\cdots(x-\beta_n) \in L[x] \tag{3}$$

We define the DISCRIMINANT $\Delta(f) \in L$ of f by

$$\Delta(f) = \alpha^{2n-2} \prod_{1\le i<j\le n} (\beta_i-\beta_j)^2 = (-1)^{n(n-1)/2}\alpha^{2n-2} \prod_{\substack{1\le i,j\le n\\ i\ne j}} (\beta_i-\beta_j). \tag{4}$$

We also define $\delta(f)$ by

$$\delta(f) = \alpha^{n-1} \prod_{1\le i<j\le n} (\beta_i-\beta_j) \in L, \tag{5}$$

so that $\delta(f)^2 = \Delta(f)$. ✌

Remark 1.3. Be aware that the quantity $\delta(f)$ from (5) is only determined up to a sign, as a different ordering of the β_i may change the factors involved in the product that defines it by a minus sign. Proposition 1.6 will describe exactly how a reordering of the zeros of f affects $\delta(f)$. ❁

Example 1.4. Suppose that $f = ax^2 + bx + c \in K[x]$ is a quadratic polynomial over a field K with $\mathrm{char}(K) \neq 2$. Then we have

$$\beta_1, \beta_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{6}$$

Therefore

$$\beta_1 - \beta_2 = \frac{\pm\sqrt{b^2 - 4ac}}{a} \tag{7}$$

and

$$\Delta(f) = a^2(\beta_1 - \beta_2)^2 = a^2\left(\frac{\sqrt{b^2 - 4ac}}{a}\right)^2 = b^2 - 4ac, \tag{8}$$

which is the usual discriminant of a quadratic polynomial. In this case the quantity $\delta(f)$ is $\pm\sqrt{b^2 - 4ac}$, with the sign depending on the chosen order of the zeros β_1, β_2 of f. ❀

To better understand the sign ambiguity in the definition of $\delta(f)$, we first prove a result on group theory that is interesting in itself.

Lemma 1.5. *Let $n \geq 2$. Then the following statements hold.*

(i) Let $\varphi : S_n \to \pm 1$ be a surjective group homomorphism. Then $\varphi = \mathrm{sgn}$.

(ii) Let $H \subset S_n$ be a subgroup of index 2. Then $H = A_n$.

Proof. (i): Let c, c' be 2-cycles in S_n. Since all such cycles are conjugate in S_n, we have $c' = \tau c \tau^{-1}$ for some $\tau \in S_n$, so that

$$\varphi(c') = \varphi(\tau c \tau^{-1}) = \varphi(\tau)\varphi(c)\varphi(\tau)^{-1} = \varphi(c)\varphi(\tau)\varphi(\tau)^{-1} = \varphi(c) \tag{9}$$

since ± 1 is abelian. We conclude that all 2-cycles in S_n have the same image under φ.

If this common image equals 1, then φ coincides with the trivial homomorphism to ± 1 on the set of 2-cycles in S_n, and since this set generates S_n, we obtain that φ in fact equals the trivial homomorphism. This is impossible because our assumption that φ be surjective. On the other hand, if the aforementioned common image equals -1, then φ coincides with the sign homomorphism on the set of 2-cycles, so that the same argument implies that $\varphi = \mathrm{sgn}$.

(ii) If H is a subgroup of index 2 in S_n, then H is normal, and it is the kernel of the canonical projection homomorphism $\pi : G \to G/H$. Since G/H is a group of order $\#(G/H) = [G : H] = 2$, it is isomorphic to ± 1. Choose an isomorphism ι and let $\varphi = \iota\pi : G \to \pm 1$. Then $\varphi = \mathrm{sgn}$ by Part (i), so that

$$H = \ker(\pi) = \ker(\iota\pi) = \ker(\varphi) = \ker(\mathrm{sgn}) = A_n. \tag{10}$$

♡

Depending on how you were raised, the upcoming result may be your definition of the sign homomorphism.

Proposition 1.6. *Let K be a field, and let $R = K[x_1, \ldots, x_n]$. Then S_n acts on R by permutation of the coordinates, and for the polynomial*

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j) \tag{11}$$

we have that $\sigma(D) = \operatorname{sgn}(\sigma) D$.

Proof. Given $\sigma \in S_n$, the universal property of polynomial rings implies that there exists a unique K-automorphism φ_σ of R such that $\varphi_\sigma(x_i) = x_{\sigma(i)}$. Moreover, for all $\sigma, \tau \in S_n$ and for all i between 1 and n we have that

$$\varphi_{\sigma\tau}(x_i) = x_{(\sigma\tau)(i)} = x_{\sigma(\tau(i))} = \varphi_\sigma(x_{\tau(i)}) = \varphi_\sigma(\varphi_\tau(x_i)) = (\varphi_\sigma \varphi_\tau)(x_i). \tag{12}$$

Since the elements $x_1, \ldots, x_n$ generate R over K, we conclude that $\varphi_{\sigma\tau} = \varphi_\sigma \varphi_\tau$, so that we indeed obtain a (left) action of S_n on R.

Since R, being a polynomial ring over a field, is an integral domain, the polynomial D is non-zero, as it is a product of non-zero factors. Moreover, if we apply the action of $\sigma \in S_n$, then all that can change is that the factors that make up D get multiplied by a minus sign. We see that

$$\sigma(D) = s(\sigma) D \tag{13}$$

for some $s(\sigma) \in \pm 1$, which is uniquely determined because D is non-zero. Now we have

$$\begin{aligned} s(\sigma\tau)D &= (\sigma\tau)(D) = \sigma(\tau(D)) = \sigma(s(\tau)D) = \sigma(s(\tau))\sigma(D) = s(\tau)\sigma(D) \\ &= s(\tau)s(\sigma)D = s(\sigma)s(\tau)D. \end{aligned} \tag{14}$$

The aforementioned uniqueness therefore allows us to conclude that

$$s(\sigma\tau) = s(\sigma)s(\tau), \tag{15}$$

for all $\sigma, \tau \in \operatorname{Gal}(L|K)$, so that the map

$$\begin{aligned} s : S_n &\to \pm 1 \\ \sigma &\mapsto s(\sigma) \end{aligned} \tag{16}$$

is a group homomorphism. Moreover, since the action (1 2) maps the pair $(1,2)$ to $(2,1)$, whereas it maps the set of all other pairs (i,j) with $i < j$ to itself, we obtain

$$(1\ 2)D = (x_2 - x_1) \prod_{\substack{\text{other } (i,j) \text{ with} \\ 1 \leq i < j \leq n}} (x_i - x_j) = -(x_1 - x_2) \prod_{\substack{\text{other } (i,j) \text{ with} \\ 1 \leq i < j \leq n}} (x_i - x_j) = -D. \tag{17}$$

Thus we see that $s((1\ 2)) = -1$, so that s is non-trivial. We can now use Lemma 1.5(i) to conclude that $s = \operatorname{sgn}$, which yields the statement of the proposition. ♡

As the following theorem shows, the fact that $\delta(f)$ may transform non-trivially when permuting the zeros $\beta_1,\dots,\beta_n$ is not a bug, but a feature.

Theorem 1.7. *Let K be a field whose characteristic does not equal 2, and let $f \in K[x]$ be a separable polynomial of degree n with splitting field $L\,|\,K$ and Galois group $G = \mathrm{Gal}(f) := \mathrm{Gal}(L|K)$. Then the following statements hold.*

(i) The discriminant $\Delta(f)$ is a non-zero element of K.

(ii) We have $G \subset A_n$ if and only if $\Delta(f)$ is a square in K.

(iii) If $\Delta(f)$ is not a square in K, then $K(\sqrt{\Delta(f)}) = K(\delta(f))$ is a quadratic extension of K; the corresponding fix group is given by the subgroup $G \cap A_n$ of G.

Proof. If we let $P \in K[x_1,\dots,x_n]$ be the polynomials from Proposition 1.6, then we have

$$\delta(f) = \alpha^{n-1} P(\beta_1,\dots,\beta_n). \tag{18}$$

Since $\alpha \neq 0$ and the β_i are mutually distinct by the separability hypothesis on f, we see that $\delta(f)$, being a product of non-zero elements of the field L, is itself non-zero, and therefore the same holds for $\Delta(f) = \delta(f)^2$.

To see that $\Delta(f)$ belongs to K, recall from Theorem 4.1(ii) that the elements σ of G act on the zeros of f. Moreover, the K-linearity of σ along with Proposition 1.6 imply that

$$\begin{aligned}\sigma(\delta(f)) &= \sigma(\alpha^{n-1}P(\beta_1,\dots,\beta_n)) = \alpha^{n-1}\sigma(P(\beta_1,\dots,\beta_n))\\ &= \alpha^{n-1}P(\sigma(\beta_1),\dots,\sigma(\beta_n)) = \alpha^{n-1}P(\beta_{\sigma(1)},\dots,\beta_{\sigma(n)})\\ &= \alpha^{n-1}(\sigma P)(\beta_1,\dots,\beta_n) = \mathrm{sgn}(\sigma)\alpha^{n-1}P(\beta_1,\dots,\beta_n)\\ &= \mathrm{sgn}(\sigma)\delta(f)\end{aligned} \tag{19}$$

and therefore also

$$\sigma(\Delta(f)) = \sigma(\delta(f)^2) = \sigma(\delta(f))^2 = (\mathrm{sgn}(\sigma)\delta(f))^2 = \delta(f)^2 = \Delta(f). \tag{20}$$

Since σ was arbitrary, Theorem III.2.3(ii) implies that $\Delta(f) \in L^G = K$, which shows (i).

(ii): We have $G \subset A_n$ if and only if $G \cap A_n = G$. Now given $\sigma \in G$, we have that $\sigma \in A_n$ if and only if $\sigma(\delta(f)) = \delta(f)$. We therefore see that $G \subset A_n$ if and only if $\delta(f)$ is fixed by all elements of G, which Theorem III.2.3(ii) shows to be the case if and only if $\delta(f) \in K$. Since the elements of L whose square equals $\Delta(f)$ are exactly $\pm\delta(f)$, this is equivalent with $\Delta(f)$ being a square in K.

(iii) An element σ of G fixes the subextension $K(\delta(f))|K$ of $L|K$ if and only if it fixes $\delta(f)$. By (19), this is the case if and only if $\sigma \in G \cap A_n$. Now $G \cap A_n$ is the kernel of the sign homomorphism sgn restricted to $G \subset S_n$, so if it is not all of G, then it is a subgroup of index 2. In this case $K(\delta(f))|K$ is a quadratic extension of K by Theorem 1.2(iii). ♡

Remark 1.8. Theorem 1.7 can be extended to characteristic 2; see Exercise 4. ❁

While Theorem 1.7 is very beautiful, we should not pat ourselves on the back yet. It is usually very difficult to write down the splitting field $L|K$ explicitly; if f is of degree $n \geq 12$ with Galois group S_n, this challenge is already insuperable for contemporary computer algebra systems. Therefore it is out of the question to obtain $\Delta(f)$ by directly evaluating (4) in the field extension $L|K$. Instead, let us consider the expression

$$\Delta(f) = \alpha^{2n-2} \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} \alpha^{2n-2} \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} (\beta_i - \beta_j) \tag{21}$$

a bit further. Since

$$f = \alpha \prod_{1 \leq i \leq n} (x - \beta_i), \tag{22}$$

repeated application of the product rule shows that the derivative f' is given by

$$f' = \alpha \sum_{1 \leq i \leq n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x - \beta_j). \tag{23}$$

In particular, we see that

$$f'(\beta_i) = \alpha \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\beta_i - \beta_j) \tag{24}$$

since all product terms in (23) for indices not equal to i contain a factor $\beta_i - \beta_i$ and therefore reduce to 0. This allows us to rewrite (21) as

$$\Delta(f) = (-1)^{n(n-1)/2} \alpha^{n-2} \prod_{1 \leq i \leq n} f'(\beta_i). \tag{25}$$

Up to the constant factor in front, we see that we are taking the product of the evaluations of f' in the zeros of f. This construction admits a generalization, explained in [Mil22, Appendix to Chapter 4], which we shall also use in a slightly adapted form.

Definition 1.9. Let K be a field, and let f and g be polynomials of strictly positive degree. If

$$f = \alpha_f \prod_{1 \leq i \leq n} (x - \beta_i) \qquad g = \alpha_g \prod_{1 \leq j \leq m} (x - \gamma_j) \tag{26}$$

in a common splitting field L of f and g, then we define the RESULTANT $\operatorname{Res}(f, g)$ of f and g as

$$\operatorname{Res}(f,g) = \alpha_f^m \alpha_g^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (\beta_i - \gamma_j) = \alpha_f^m \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \alpha_g (\beta_i - \gamma_j) = \alpha_f^m \prod_{1 \leq i \leq n} g(\beta_i). \tag{27}$$

If either f or g is the zero polynomial, then we define $\operatorname{Res}(f, g) = 0$; otherwise we define

$$\operatorname{Res}(f,g) = \alpha_f^m, \quad \text{respectively} \quad \operatorname{Res}(f,g) = \alpha_g^n \tag{28}$$

if $f = \alpha_f$, respectively $g = \alpha_g$ is constant; this amounts to taking the empty product in (27) equal to 1. Note that the definitions in (28) are compatible when f and g are both non-zero constants, as we then have $\mathrm{Res}(f,g) = 1$ in either case. ✌

Definition 1.9 involves a choice of common splitting field, and a priori this might affect the definition of $\mathrm{Res}(f,g)$. That this problem does not in fact arise is a consequence of the following proposition.

Proposition 1.10. *Let K be a field, and let $f, g \in K[x]$ be of degree n and m, respectively. Then the following properties hold.*

(i) $\mathrm{Res}(f,g) = (-1)^{mn}\mathrm{Res}(g,f)$.

(ii) $\mathrm{Res}(\lambda f, g) = \lambda^m \mathrm{Res}(f,g)$ *and* $\mathrm{Res}(f,\lambda g) = \lambda^n \mathrm{Res}(f,g)$ *for* $\lambda \in K$.

(iii) If $g = qf + r$ *and* $\deg(r) = \ell$, *then*

$$\mathrm{Res}(f,g) = \alpha^{m-\ell}\mathrm{Res}(f,r). \tag{29}$$

(iv) $\mathrm{Res}(f,g)$ *is an element of* K.

Proof. (i): If $n > 0$ and $m > 0$, then we have

$$\mathrm{Res}(f,g) = \alpha_f^m \alpha_g^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_i - \gamma_j) = \alpha_g^n \alpha_f^n \prod_{\substack{1\le j\le m\\ 1\le i\le n}} (\gamma_j - \beta_i) = (-1)^{mn}\mathrm{Res}(g,f), \tag{30}$$

where the middle equality is a consequence of the fact that mn sign switches from $\beta_i - \gamma_j$ to $\gamma_j - \beta_i$ were performed. As these equalities also hold if the products involved are empty, it remains to consider the case when either f or g is zero, but then both sides of the desired equality are 0.

(ii): If $n > 0$ and $m > 0$, then we have

$$\mathrm{Res}(\lambda f, g) = (\lambda\alpha_f)^m \alpha_g^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_i - \gamma_j) = \lambda^m \alpha_f^m \alpha_g^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_i - \gamma_j) = \lambda^m \mathrm{Res}(f,g) \tag{31}$$

and

$$\mathrm{Res}(f,\lambda g) = \alpha_f^m (\lambda\alpha)_g^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_i - \gamma_j) = \lambda^n \alpha_f^m \alpha_g^n \prod_{\substack{1\le i\le n\\ 1\le j\le m}} (\beta_i - \gamma_j) = \lambda^n \mathrm{Res}(f,g). \tag{32}$$

As these equalities also hold if the products involved are empty, it remains to consider the case when either f or g is zero, but then both sides of the desired equalities are 0.

(iii): If $f = 0$, then both sides of (29) equal 0, and if $f = \alpha$ is constant, then it amounts to the equality $\alpha^m = \alpha^{m-\ell}\alpha^\ell$. Otherwise let us write $r = \sigma\prod_{k=1}^{\ell}(x - \tau_k)$. Then since $f(\beta_i) = 0$ for all i between 1 and n, we obtain the chain of equalities

$$\begin{aligned}\mathrm{Res}(f,g) &= \alpha^m \prod_{1\le i\le n} g(\beta_i) = \alpha^m \prod_{1\le i\le n} (q(\beta_i)f(\beta_i) + r(\beta_i))\\ &= \alpha^m \prod_{1\le i\le n} r(\beta_i) = \alpha^{m-\ell}\alpha^\ell \prod_{1\le i\le n} r(\beta_i)\\ &= \alpha^{m-\ell}\mathrm{Res}(f,r).\end{aligned} \tag{33}$$

We have to be careful with the final equality in (33) when r is constant; but if $r = 0$, then both sides equal 0, and if $r = \gamma$ is another constant, then the equality amounts to $\alpha^{m-0}\alpha^0\gamma^n = \alpha^{m-0}\gamma^n$.

(iv): Parts (i)-(iii) show that given $f, g \in K[x]$, the resultant can be calculated by repeated division with remainder for polynomials, which can be performed over the base field K. In the end, one of f or g will be either linear or constant, at which point we can either directly evaluate (27) or invoke the corner case (28). Either way, we obtain a result in the base field K. ♡

Remark 1.11. (i) The virtue of Proposition 1.10 is the fact that division with remainder is a highly efficient algorithms that can be performed over the base field K, and that obviates the need for any actual calculation of the zeros of f and g. We have therefore resolved the issue that motivated our closer look at the resultant.

(ii) The properties in Proposition 1.10(i)-(iii), along with the corner cases when f and g are constant, characterize the resultant $\mathrm{Res}(f, g)$. This can be used to show that it can be computed by means of a matrix as well; see Exercise 5. ❁

As the following Proposition shows, there is a small change in the constant factor when describing the discriminant as a resultant.

Proposition 1.12. *Let $f \in K[x]$ be a non-constant polynomial of degree n with leading coefficient α. Then we have*

$$\Delta(f) = (-1)^{n(n-1)/2}\alpha^{-1}\,\mathrm{Res}(f, f') \in K. \tag{34}$$

Proof. Let us write

$$f = \alpha\prod_{i=1}^{n}(x - \beta_i) \tag{35}$$

over a splitting field L of f. By the definition of the resultant, we have

$$\mathrm{Res}(f, f') = \alpha^{n-1}\prod_{1\le i\le n} f'(\beta_i). \tag{36}$$

Since (25) showed that

$$\Delta(f) = (-1)^{n(n-1)/2}\alpha^{n-2}\prod_{1\le i\le n} f'(\beta_i). \tag{37}$$

we obtain (34) by comparison. ♡

Remark 1.13. In [Mil22, Proposition 4.36] it is claimed that we also have

$$\Delta(f) = (-1)^{n(n-1)/2}\alpha^{-1}\,\mathrm{Res}(f', f) \in K. \tag{38}$$

This statement is incorrect, as it amounts to the equality $\mathrm{Res}(f, f') = \mathrm{Res}(f', f)$. In light of 1.10(i), this does not hold if $\deg(f)$ and $\deg(f')$ are both odd, as happens for the separable irreducible cubic polynomial

$$x^3 + x^2 - 1 \in \mathbb{F}_3[x]. \tag{39}$$

❁

Example 1.14. (i) Let $a, b \in K$ for a field K whose characteristic does not equal 2 or 3, and consider the cubic polynomial $f = x^3 + ax + b \in K[x]$. Then the derivative $f' = 3x^2 + a$ is of degree 2, so by applying Proposition 1.12 and the properties (i)-(iii) in Proposition 1.10 we obtain

$$\begin{aligned}
\mathrm{Disc}(f) &\overset{1.12}{=} -\mathrm{Res}(f, f') \overset{(i)}{=} -\mathrm{Res}(f', f) \\
&= -\mathrm{Res}(3x^2 + a, x^3 + ax + b) \overset{(ii)}{=} -3^3 \mathrm{Res}(x^2 + \frac{1}{3}a, x^3 + ax + b) \\
&= -3^3 \mathrm{Res}(x^2 + \frac{1}{3}a, x(x^2 + \frac{1}{3}a) + \frac{2}{3}ax + b) \\
&\overset{(iii)}{=} -3^3 \mathrm{Res}(x^2 + \frac{1}{3}a, \frac{2}{3}ax + b) \overset{(i)}{=} -3^3 \mathrm{Res}(\frac{2}{3}ax + b, x^2 + \frac{1}{3}a) \\
&\overset{(ii)}{=} -3^3 \left(\frac{2a}{3}\right)^2 \mathrm{Res}(x + \frac{3b}{2a}, x^2 + \frac{1}{3}a) \\
&\overset{(27)}{=} -3^3 \left(\frac{2a}{3}\right)^2 \left(\left(\frac{-3b}{2a}\right)^2 + \frac{a}{3}\right) = -3^3 \frac{4a^2}{3^2} \frac{27b^2 + 4a^3}{12a^2} \\
&= -4a^3 - 27b^2.
\end{aligned} \tag{40}$$

Note that this computation involved division by a. However, it remains valid when $a = 0$, as also in this case we obtain

$$\begin{aligned}
\mathrm{Disc}(f) &\overset{1.12}{=} -\mathrm{Res}(f, f') \overset{(i)}{=} -\mathrm{Res}(f', f) \\
&= -\mathrm{Res}(3x^2, x^3 + b) \overset{(ii)}{=} -3^3 \mathrm{Res}(x^2, x^3 + b) \\
&\overset{(27)}{=} -3^3(0 + b)^2 = -27b^2 = -4a^3 - 27b^2.
\end{aligned} \tag{41}$$

Moreover, if $\mathrm{char}(K) = 3$, then if $a = 0$ we obtain $f' = 0$, so that f has a triple zero and $\mathrm{Disc}(f) = 0$. Otherwise $f' = a$ is of degree 1, so that

$$\begin{aligned}
\mathrm{Disc}(f) &\overset{1.12}{=} -\mathrm{Res}(f, f') \overset{(i)}{=} -\mathrm{Res}(f', f) \\
&= -\mathrm{Res}(a, x^3 + ax + b) \overset{(28)}{=} -a^3 = -4a^3 - 27b^2.
\end{aligned} \tag{42}$$

Finally, if $\mathrm{char}(K) = 2$, then

$$\begin{aligned}
\mathrm{Disc}(f) &\overset{1.12}{=} \mathrm{Res}(f, f') \overset{(i)}{=} \mathrm{Res}(f', f) \\
&= \mathrm{Res}(x^2 + a, x^3 + ax + b) = \mathrm{Res}(x^2 + a, x(x^2 + a) + b) \\
&\overset{(iii)}{=} \mathrm{Res}(x^2 + a, b) \overset{(28)}{=} b^2 = -4a^3 - 27b^2.
\end{aligned} \tag{43}$$

We see that the formula

$$\Delta(f) = -4a^3 - 27b^2 \tag{44}$$

for the discriminant of a cubic polynomial $f = x^3 + ax + b$ with trivial quadratic term is universally valid. Of course there are deeper reasons for this than the case distinction above...

(ii) A calculation shows that for the polynomial

$$f = x^4 - x - 1 \in \mathbb{Q}[x] \tag{45}$$

we have $\Delta(f) = -283$. Therefore Theorem 1.7(iii) shows that the splitting field of f (though not its stem field; also see Exercise IV.11) contains the quadratic subfield $\mathbb{Q}(\sqrt{-283})$. This result is impossible to eyeball from the polynomial f itself and therefore shows how useful the discriminant is. ❀

Combining Proposition 1.1, Theorem 1.7 and Example 1.14(i), we obtain the following result for a special class of cubic polynomials.

Theorem 1.15. *Let K be a field whose characteristic does not equal 2, and let f be a separable irreducible cubic polynomial with splitting field $L|K$. As in Theorem III.4.1, we identify G with a subgroup of S_3 via a labeling of the zeros of f.*

Let Δ be the discriminant of f, so that in particular $\Delta = -4a^3 - 27b^2$ when $f = x^3 + ax + b$ for some $a, b \in K$. Then the following statements hold.

(i) If Δ is a square in K, then $\mathrm{Gal}(f) \simeq A_3$. Moreover, the splitting field $L|K$ is a cubic extension of K, and it equals the stem field of f.

(ii) If Δ is not a square in K, then $\mathrm{Gal}(f) \simeq S_3$. Moreover, the splitting field $L|K$ is sextic extension of K, and it is the compositum of the stem field of K with the unique quadratic subextension $K(\sqrt{\Delta})|K$ of $L|K$.

Proof. The only remaining statement to be shown is that on the compositum in Part (ii). Let $\beta_1, \beta_2, \beta_3$ be the zeros of f in L. The extension $K(\beta_1)$ is isomorphic to the stem field of K, and as in Example III.1.3(iii) we see that the corresponding subgroup of S_3 is $H = \langle (2\ 3) \rangle$. On the other hand, the subextension $K(\sqrt{D})$ corresponds to the subgroup $N = A_3$ of S_3 by Theorem 1.7(iii). Since $H \cap N = \{e\}$, we see that L is the compositum of $K(\beta_1)$ and $K(\sqrt{D})$ by Theorem IV.3.3(i). ♡

Example 1.16. (i) Let $f = x^3 - 2 \in \mathbb{Q}[x]$. Then $\Delta(f) = -108$. As this is not a square in $\mathbb{Q}$, Theorem 1.15 implies that $\mathrm{Gal}(f) \simeq S_3$, a fact that we have seen many times before in different guises.

(ii) Let $f = x^3 - x^2 - 2x + 1 \in \mathbb{Q}[x]$ be the polynomial from Example I.1.9(ii). Then a direct computation using Proposition 1.10 shows that $\Delta(f) = 49$. Since this is a square in $\mathbb{Q}$, Theorem 1.15 implies that the stem field $K = \mathbb{Q}[x]/(f)$ is a cubic Galois extension of $\mathbb{Q}$. In particular, we obtain that K is normal, so that f splits into linear factors over K by Corollary I.1.13, a fact that we saw explicitly in Example I.1.9(ii) itself.

Note that K is equally well defined by the polynomial $g = f(x + 1/3) = x^3 - (7/3)x + (7/27)$. The discriminant of this polynomial can be calculated by means of the formula from Example 1.4(i), and it again equals 49.

(iii) It can be shown that the polynomial $f = x^3 - x - 1 \in \mathbb{Q}[x]$ is irreducible. As a computation shows that $\Delta(f) = -23$, Theorem 1.15 implies that $\mathrm{Gal}(f) \simeq S_3$, a special case of the statement at the end of the introduction to this chapter. ❀

The existence of the discriminant may seem like a bizarre stroke of luck, but nothing could be further from the truth. We will generalize the principles that underlie its construction in the upcoming section, as well as in Section VII.1.

2 Methods for degree 4

In analogy with the start of the previous section, we start our analysis of the possible Galois groups of separable irreducible quartic polynomials by classifying the transitive subgroups of the symmetric group S_4.

Proposition 2.1. *Let $G \subset S_4$ be a transitive subgroup. Then exactly one of the following possibilities holds.*

(i) *G is conjugate to $\langle (1\ 2\ 3\ 4) \rangle \simeq C_4$.*

(ii) *G is conjugate to $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle =: V_4$.*

(iii) *G is conjugate to $\langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle \simeq D_4$.*

(iv) *$G = A_4$.*

(v) *$G = S_4$.*

*Proof**. As in the proof of Proposition 1.1, we see that $4 \mid \#G \mid 4! = 24$. First suppose that we also have $3 \mid \#G$, so that $\#G \in \{12, 24\}$. By Cauchy's theorem, G contains an element τ of order 3, and in S_4 the only such elements are 3-cycles. After renumbering, we may assume that $\tau = (1\ 2\ 3)$. Taking powers, we see that G also contains the 3-cycle $(1\ 3\ 2)$. Moreover, since G is transitive, there exists some element σ that maps 3 to 4. We thus obtain another 3-cycle

$$\tau' = \sigma\tau\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3)) = (\sigma(1)\ \sigma(2)\ 4). \tag{46}$$

as well as its inverse $(\sigma(2)\ \sigma(1)\ 4)$. The first two entries in these representations of τ' and $(\tau')^{-1}$ belong to $\{1, 2, 3\}$. We see that if we conjugate these two 3-cycles by powers of τ, we obtain that G contains all of the 3-cycles

$$(1\ 2\ 4), \quad (2\ 1\ 4), \quad (1\ 3\ 4), \quad (3\ 1\ 4), \quad (2\ 3\ 4), \quad (3\ 2\ 4). \tag{47}$$

in A_4, and therefore all 3-cycles in this group, since we already saw that it contains $(1\ 2\ 3)$ and its inverse $(1\ 3\ 2)$. Since A_4 is generated by its 3-cycles, we conclude that G contains A_4, and since $S_4/A_4 \simeq C_2$, the subgroup correspondence induced by Noether's isomorphism theorem shows that G is either A_4 or S_4. Note that this conclusion is not affected by our choice of renumbering at the beginning of this step, as this only affects G by a conjugation in S_4, which leaves said group invariant since both A_4 and S_4 are normal in S_4.

We may therefore assume that $\#G \in \{4, 8\}$. Now suppose that G contains a 2-cycle τ, which we may assume to equal $(1\ 3)$ after renumbering. By transitivity of G, there exists an element $\sigma \in G$ that maps some element of the subset $\{1, 3\}$ of $\{1, 2, 3, 4\}$ outside of it. Conjugating τ accordingly, we therefore obtain another 2-cycle

$$\tau' = \sigma\tau\sigma^{-1} = (\sigma(1)\ \sigma(2)) = (\sigma(1)\ \sigma(2)). \tag{48}$$

If the supports of the 2-cycles τ and τ' overlap, then $\tau\tau'$ is a 3-cycle, which in light of Lagrange's theorem leads to a contradiction on our hypothesis on the cardinality of G. We may therefore assume that σ maps $\{1,3\}$ to $\{2,4\}$, and by renumbering the elements of the latter set if necessary, we may assume that $\sigma(1) = 2$ and $\sigma(3) = 4$. This leads to the two possibilities $\sigma = (1\ 2)(3\ 4)$ and $\sigma = (1\ 2\ 3\ 4)$.

If $\sigma = (1\ 2)(3\ 4)$, then upon conjugating σ by τ we obtain the element $\sigma' = (1\ 4)(2\ 3)$. Therefore G contains the normal subgroup $V_4 = \{e, \sigma, \sigma', \sigma\sigma'\}$, and this time the subgroup correspondence for $G/V_4 \simeq S_3$ shows that G is an inverse image of one of the subgroups of S_3. Now we know that $\#(G/V_4) = \#G/\#V_4 \in \{4/4, 8/4\} = \{1,3\}$, so since G/V_4 contains the image $\langle 1\ 2\rangle V_4$, which is of order 2, we must in fact have

$$G = \langle (1\ 3)\rangle V_4 = \{e, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3), (2\ 4), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4)\}. \tag{49}$$

While this argument depends on our choice of numbering to obtain $\tau = (1\ 3)$, the other possibilities lead to conjugate subgroups of S_4.

We may therefore suppose that G contains neither 2-cycles nor 3-cycles. If G does not contain any 4-cycles either, then G can only contain the identity element and $(2,2)$-cycles, that is, the three elements of V_4. In particular, this implies that $\#G \leq 4$. Since we already saw that $\#G \geq 4$, we can conclude that $G = V_4$ in this case.

Finally, if G contains a 4-cycle σ, then we may assume that $\sigma = (1\ 2\ 3\ 4)$ up to renumbering. Then G also contains $\sigma^2 = (1\ 3)(2\ 4)$. If G contains another $(2,2)$-cycle, then it contains all of V_4 and therefore corresponds to one of the subgroups G that is obtained by lifting the subgroups of $G/V_4 \simeq S_4$ under the canonical projection, but we have already found all such subgroups above; the inverse image of the trivial subgroup equals V_4, that of the full subgroup equals S_4, that of A_3 equals A_4, and the inverse images of the remaining 3 subgroups of order 2 are the conjugates of (49). The only remaining possibility is then that G is generated by σ; otherwise G would contain a 4-cycle that is not a power of σ, but such 4-cycles all have a square that is a $(2,2)$-cycle distinct from σ^2, and we just concluded that we already covered these cases. Also in this final case, a different renumbering only changes G by a conjugation inside S_4. ♡

It now remains to decide, given a separable irreducible polynomial $f \in K[x]$, to which of the five groups in Proposition 2.1 the group $\mathrm{Gal}(f)$ is isomorphic. Provided that we are in characteristic not equal to 2, Theorem 1.7 still gives a criterion for $\mathrm{Gal}(f)$ to be contained in A_4, but in degree 4 this is not enough. The next largest group in Proposition 2.1 that we should consider is

$$H_2 := \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4)\rangle \simeq D_4. \tag{50}$$

This is the group of symmetries of a square, and we should try to see what special properties it satisfies in order to construct a suitable analogue of the discriminant for this group.

Now in whatever way we rotate or reflect the square, a pair of vertices that are opposite to one another will always be mapped to a pair of vertices with the same property. If we therefore subdivide the vertices of the square

accordingly, then the action of D_4 will preserve this partition (even though it may not preserve the individual subsets making up this partition). For the group H_2 from (50), which describes the group of symmetries of the square with vertices labeled $1,2,3,4$ counterclockwise, said partition into pairs of opposite vertices is given by $\{\{1,3\},\{2,4\}\}$, and this is indeed stable under the generators $r := (1\ 2\ 3\ 4)$ and $s = (1\ 2)(3\ 4)$ of G, since

$$\begin{aligned} \{r(1), r(3)\} &= \{2,4\} \in \{\{1,2\},\{3,4\}\}, \\ \{r(2), r(4)\} &= \{3,1\} \in \{\{1,2\},\{3,4\}\}, \\ \{s(1), s(3)\} &= \{2,1\} \in \{\{1,2\},\{3,4\}\}, \\ \{s(2), s(4)\} &= \{4,3\} \in \{\{1,2\},\{3,4\}\}. \end{aligned} \tag{51}$$

Another (equivalent) way to look at this phenomenon is the following. Conjugation induces an action of S_4 on its normal subgroup V_4, and since any conjugation maps the identity permutation to itself, we also obtain an action on the subset

$$X = V_4 - \{e\} = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \tag{52}$$

In other words, we have constructed a group homomorphism

$$\begin{aligned} \rho : S_4 &\to \mathrm{Sym}(X), \\ \sigma &\mapsto (x \mapsto \sigma x \sigma^{-1}). \end{aligned} \tag{53}$$

Because all $(2,2)$-cycles in S_4 are conjugate, the action ρ is in fact transitive. The orbit-stabilizer theorem therefore shows that the stabilizers of the various elements of X have cardinality $\#G/\#X = 24/3 = 8$. Now our above argumentation shows that H_2 stabilizes the element $(1\ 3)(2\ 4)$ under conjugation, so since $\#H_2$ is of cardinality 8, we obtain

$$H_2 := \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) = S^\rho((1\ 3)(2\ 4)). \tag{54}$$

Similarly, we obtain yet two more subgroups of S_4 that arise from a relabeling of the vertices of the square, namely

$$\begin{aligned} H_1 &:= \langle (1\ 3\ 2\ 4), (1\ 3)(2\ 4) = S^\rho((1\ 2)(3\ 4)) \quad \text{and} \\ H_3 &:= \langle (1\ 2\ 4\ 3), (1\ 2)(4\ 3) = S^\rho((1\ 4)(2\ 3)). \end{aligned} \tag{55}$$

Proposition 2.2. *Let $H \subset S_4$ be a subgroup that is isomorphic to D_4. Then H is one of the subgroups H_1, H_2 and H_3 from (54) and (55).*

Proof. Proposition 2.1 shows that such a group H is conjugate in S_4 to the group H_2. If we now consider the conjugation action of S_4 on its subgroups, then certainly H_2 is stabilized by itself. Therefore the length of its orbit is at most $\#[G : H_2] = \#(G/H_2) = \#G/\#H_2 = 24/8 = 3$. On the other hand, we already saw that H_1, H_2 and H_3 are in the orbit of H under conjugation. They therefore constitute the full orbit, and therefore H equals one of them. ♡

The other transitive subgroups of S_4 can in fact be characterized in terms of their inclusions in A_4 and the subgroups H_1, H_2, H_3, as Proposition 2.1 has the following corollary.

Corollary 2.3. *Let $G \subset S_4$ be a transitive subgroup. Then the following statements hold.*

(i) If $G \simeq C_4$, then $G \not\subset A_4$ and $G \subset H_i$ for a unique $i \in \{1,2,3\}$.

(ii) If $G = V_4$, then $G \subset A_4$ and $G \subset H_i$ for all $i \in \{1,2,3\}$.

(iii) If $G \simeq D_4$, then $G \not\subset A_4$ and $G \subset H_i$ for a unique $i \in \{1,2,3\}$.

(iv) If $G = A_4$, then $G \subset A_4$ and $G \not\subset H_i$ for all $i \in \{1,2,3\}$.

(v) If $G = S_4$, then $G \not\subset A_4$ and $G \not\subset H_i$ for a unique $i \in \{1,2,3\}$.

Corollary 2.3 is almost enough to identify a given transitive subgroups G of S_4 up to conjugacy, except that it cannot tell C_4 and D_4 apart. Let us leave aside this subtlety for now; at the very least, we see that if, given a subgroup $G = \mathrm{Gal}(f)$ of S_4, we can develop a tool to prove the existence of inclusions $G \subset H_i$, then we will have almost reached our goal of determining the Galois groups of f explicitly.

To this end, we construct algebraic expressions in the zeros of f that have the groups H_i as their stabilizers. Let $L|K$ be the splitting field of f. Choose a labeling of the zeros $\beta_1, \ldots, \beta_4$ of f in L, and interpret $G = \mathrm{Gal}(f)$ as a subgroup of S_4 accordingly. We construct the elements

$$\begin{aligned} \gamma_1 &= \beta_1\beta_2 + \beta_3\beta_4, \\ \gamma_2 &= \beta_1\beta_3 + \beta_2\beta_4, \\ \gamma_3 &= \beta_1\beta_4 + \beta_2\beta_3 \end{aligned} \tag{56}$$

of L. Now if $\sigma \in G$ is an element of H_2, then σ fixes γ_2, as this element is invariant under the symmetries that fix the partition $\{\{1,2\},\{3,4\}\}$ of $\{1,2,3,4\}$. Explicitly, if $\sigma = r$, then we have

$$\sigma(\gamma_2) = \beta_{r(1)}\beta_{r(3)} + \beta_{r(2)}\beta_{r(4)} = \beta_2\beta_4 + \beta_3\beta_1 = \gamma_2, \tag{57}$$

whereas if $\sigma = s$, then we obtain

$$\sigma(\gamma_2) = \beta_{s(1)}\beta_{s(3)} + \beta_{s(2)}\beta_{s(4)} = \beta_2\beta_4 + \beta_1\beta_3 = \gamma_2. \tag{58}$$

Since $H_2 = \langle r, s\rangle$, we conclude that $G \cap H_2$ stabilizes γ_2. Similarly, we see that $G \cap H_1$ stabilizes γ_1 and that $G \cap H_3$ stabilizes γ_3. Now if we indeed have

$$S(\gamma_i) = G \cap H_i, \tag{59}$$

then we can hope to use Galois theory to characterize the inclusion $G \subset H_i$ in terms of stabilizing the element γ_i, and we shall do so formally in Corollary 2.5.

However, it is important to note that we have **not** proved (59) yet, though this may seem so at first sight. The reason is that the stabilizers $S(\gamma_i)$ might strictly contain H_i. In particular, this would be the case if two or more of the elements γ_i were identical, so that their common value would have a stabilizer that contains more than one of the H_i. Fortunately one can show in this particular case that this merging behavior can never happen.

Proposition 2.4. *Let $f \in K[x]$ be a separable quartic polynomial, let $L \mid K$ be a splitting field of f, let $\beta_1, \dots, \beta_4$ be the zeros of f in L, and define $\gamma_1, \gamma_2, \gamma_3$ as in (56). Then we have $\gamma_i \neq \gamma_j$ for $i \neq j$.*

Proof. We have

$$\begin{aligned} \gamma_1 - \gamma_2 &= \beta_1\beta_2 + \beta_3\beta_4 - \beta_1\beta_3 - \beta_2\beta_4 = (\beta_1 - \beta_4)(\beta_2 - \beta_3), \\ \gamma_1 - \gamma_3 &= \beta_1\beta_2 + \beta_3\beta_4 - \beta_1\beta_4 - \beta_2\beta_3 = (\beta_1 - \beta_3)(\beta_2 - \beta_4), \\ \gamma_2 - \gamma_3 &= \beta_1\beta_3 + \beta_2\beta_4 - \beta_1\beta_4 - \beta_2\beta_3 = (\beta_1 - \beta_2)(\beta_3 - \beta_4). \end{aligned} \tag{60}$$

Since L is a field, it is also an integral domain, so that if one of the differences $\gamma_i - \gamma_j$ in (60) equals 0, then $\beta_k - \beta_\ell = 0$ for some $k \neq \ell$, which is in contradiction with the hypothesis that f be separable. ♡

Corollary 2.5. *In the situation of Proposition 2.4, let $G = \mathrm{Gal}(f) = \mathrm{Gal}(L \mid K)$, considered as a subgroup of S_4 via the chosen labeling of the zeros of f. If $i \in \{1, 2, 3\}$, then $G \subset H_i$ if and only if $\gamma_i \in K$.*

Proof. Let us start by showing that the stabilizer $S(\gamma_i)$ of $\gamma_i \in L$ under the action of G is given by $G \cap H_i$. We have already seen that $H_i \subset S(\gamma_i)$. Now if $\sigma \in G$ is such that $\sigma \notin H_i$, then the proof of Proposition 2.2 implies that σ sends the partition of $\{1, 2, 3, 4\}$ that corresponds to γ_i to a different partition. Proposition 2.4 then implies that σ does not fix γ_i. We therefore obtain the desired reverse inclusion $S(\gamma_i) \subset G \cap H_i$.

Since $K = L^G$ by Theorem III.2.3(ii), we have $\gamma_i \in K$ if and only if γ_i is fixed under all elements of the group G. This is the case if and only if $G \subset G \cap H_i$, that is, if and only if $G \subset H_i$. ♡

Because of Corollary 2.3, the combination of Theorem 1.7(ii) and Corollary 2.5 gives us enough information to decide what the Galois group of a given separable quartic polynomial $f \in K[x]$, unless $\mathrm{Gal}(f)$ is either groups C_4 or D_4, in which case we shall have to use a complementary method. Regardless, we can now give our main new tool a name.

Definition 2.6. Let $f \in K[x]$ be a separable quartic polynomial, let $L \mid K$ be a splitting field of K, and write

$$f = \alpha(x - \beta_1) \cdots (x - \beta_4) \in L[x]. \tag{61}$$

We define the RESOLVENT CUBIC $\rho(f)$ of f to be the polynomial

$$\rho(f) = (x - \gamma_1)(x - \gamma_2)(x - \gamma_3) \in L[x] \tag{62}$$

where the γ_1, γ_2, γ_3 are as defined in (56). ✌

Remark 2.7. Historically, the resolvent cubic was used to reduce the solution of quartic equations by means of radicals to cubic equations. This turned out no longer to be possible from degree 5 onward, as the resolvents thus constructed were of larger degree than that of the original polynomial. We now know that there is a good reason why this should be so, but this is another phenomenon that requires Galois-theoretic methods (which we do not develop here) for a satisfactory understanding. ❁

As for the discriminant $\Delta(f)$, one can show that the resolvent cubic of f is defined over the base field K.

Proposition 2.8. *Let $f \in K[x]$ be a separable quartic polynomial. Then $\rho(f) \in K[x]$.*

Proof. We know that the Galois group of f acts on the zeros β_i by permutation of the indices; it therefore also acts the partitions of the indices $\{1,2,3,4\}$ into two pairs of two elements. As we have seen, these partitions can be associated to the γ_i in a natural way, namely by

$$\begin{aligned} (1\ 2)(3\ 4) &\leftrightarrow \beta_1\beta_2 + \beta_3\beta_4 = \gamma_1, \\ (1\ 3)(2\ 4) &\leftrightarrow \beta_1\beta_3 + \beta_2\beta_4 = \gamma_2, \\ (1\ 4)(2\ 3) &\leftrightarrow \beta_1\beta_4 + \beta_2\beta_3 = \gamma_3, \end{aligned} \tag{63}$$

In particular, we see that the Galois group of f maps the set of zeros $\{\gamma_1, \gamma_2, \gamma_3\} \subset L$ of $\rho(f)$ to itself. Since $\rho(f) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$, it is therefore itself fixed by the action of G on the polynomial ring $L[x]$. Expressed differently, this means that all the coefficients of $\rho(f)$ belong to L^G. Since the latter field equals K by Theorem III.2.3(ii), we obtain the desired result. ♡

We now have the tools required for the main theorem.

Theorem 2.9. *Let K be a field with $\mathrm{char}(K) \neq 2$, let $f \in K[x]$ be a separable irreducible quartic polynomial with discriminant Δ and resolvent cubic ρ. Then the following statements hold.*

(i) If Δ is not a square in K and ρ has no zero in K, then $\mathrm{Gal}(f) \simeq S_4$.

(ii) If Δ is a square in K and ρ has no zero in K, then $\mathrm{Gal}(f) \simeq A_4$.

(iii) If Δ is not a square in K, and ρ has a single zero in K, and f does not split into linear factors over its stem field, then $\mathrm{Gal}(f) \simeq D_4$.

(iv) If Δ is not a square in K, and ρ has a single zero in K, and f splits into linear factors over its stem field, then $\mathrm{Gal}(f) \simeq C_4$.

(v) If Δ is a square in K and ρ has three zeros in K, then $\mathrm{Gal}(f) \simeq V_4$.

Proof. This statement follows from Corollary 2.3 in combination with Theorem 1.7(ii) and Corollary 2.5, except for the case distinction between D_4 and C_4.

To see this final part, we use Corollary I.1.13 and Theorem I.1.6. If $G \simeq C_4$, the quartic stem field of the separable polynomial f is already the splitting field of f over K, and therefore a Galois extension of K, whereas if $G \simeq D_4$, the splitting field of f is an extension of its stem field of degree $\#D_4/4 = 8/2 = 4$, so that f cannot split into linear factors over it. ♡

Remark 2.10. There is another possible method to distinguish Cases (iv) and (v) in Theorem 2.9, which can be found in [Mil22, Chapter 4]: If $\mathrm{Gal}(f) \simeq D_4$, then f is irreducible over the quadratic splitting field of ρ, whereas f is a product of quadratic factors over this splitting field if $\mathrm{Gal}(f) \simeq C_4$.

That said, either criterion involves a certain amount of disingenuous hand-waving, since at this point you will most likely not have seen explicit criteria for finding zeros or for determining irreducible factors of polynomials over general fields. We simply confess a lack of knowledge in this regard and refer to a course on algorithmic algebra for developing such methods. ❁

As for the discriminant, it is in general inefficient first to calculate the splitting field of f and its roots $\beta_1,\dots,\beta_4$ explicitly do determine $\rho(f)$. Instead, it again turns out that calculating $\rho(f)$ is possible over the ground field K.

Proposition 2.11. *Let*

$$f = a(x^4 + a_1x^3 + a_2x^2 + a_3x + a_4) \in K[x]. \tag{64}$$

Then we have

$$\rho(f) = x^3 - a_2x^2 + (a_1a_3 - 4a_4)x - a_1^2a_4 - a_3^2 + 4a_2a_4. \tag{65}$$

Proof. Writing out $\rho(f) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3)$ after substituting (56), we obtain that

$$\begin{aligned}\rho(f) = x^3 &- (\beta_1\beta_2 + \beta_1\beta_3 + \beta_1\beta_4 + \beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4)x^2\\ &+ (\beta_1^2\beta_2\beta_3 + \beta_1^2\beta_2\beta_4 + \beta_1^2\beta_3\beta_4 + \beta_1\beta_2^2\beta_3 + \beta_1\beta_2^2\beta_4 + \beta_1\beta_2\beta_3^2\\ &\quad + \beta_1\beta_2\beta_4^2 + \beta_1\beta_3^2\beta_4 + \beta_1\beta_3\beta_4^2 + \beta_2^2\beta_3\beta_4 + \beta_2\beta_3^2\beta_4 + \beta_2\beta_3\beta_4^2)x\\ &- (\beta_1^3\beta_2\beta_3\beta_4 + \beta_1^2\beta_2^2\beta_3^2 + \beta_1^2\beta_2^2\beta_4^2 + \beta_1^2\beta_3^2\beta_4^2\\ &\quad + \beta_1\beta_2^3\beta_3\beta_4 + \beta_1\beta_2\beta_3^3\beta_4 + \beta_1\beta_2\beta_3\beta_4^3 + \beta_2^2\beta_3^2\beta_4^2).\end{aligned} \tag{66}$$

For $i = 1,\dots,4$, let us consider the symmetric expressions $s_i = s_i(\alpha_1,\dots,\alpha_4)$ in the roots of f. Then Example 3.4(i)-(iii) shows that

$$\rho(f) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - s_1^2s_4 - s_3^2 + 4s_2s_4, \tag{67}$$

so that the statement of the Proposition is a consequence of Example 3.4(iv), which shows that $s_i = (-1)^i a_i$. ♡

We now have everything that we need to start cranking out examples.

Example 2.12. (i) Let $f = x^4 - x - 1 \in \mathbb{Q}[x]$. Then $\Delta(f)$ equals the non-square -283, as we saw in Example 1.14(ii), whereas the polynomial

$$\rho(f) = x^3 + 4x - 1 \in \mathbb{Q}[x] \tag{68}$$

has no zeros in $\mathbb{Q}$. Indeed, since $\rho(f)$ is integral, the only possible zeros are of the form a/b, where a divides the constant term -1 of f and where b divides the leading coefficient 1 of f. The only fractions a/b obtained in this way are ±1, which are not in fact zeros of $\rho(f)$. We therefore see that $\mathrm{Gal}(f) \simeq S_4$.

(ii) Let $f = x^4 - 2x^3 + 2x^2 + 2 \in \mathbb{Q}[x]$. Then $\Delta(f) = 3136 = 56^2$, whereas

$$\rho(f) = x^3 - 2x^2 - 8x + 8. \tag{69}$$

Since none of the a priori possible zeros $\pm1, \pm2, \pm4, \pm8$ of $\rho(f)$ are in fact zeros, we conclude that $\mathrm{Gal}(f) \simeq A_4$.

(iii) Let $f = x^4 - x^3 - x^2 + x + 1 \in \mathbb{Q}[x]$. Then $\Delta(f) = 117$ is not a square, whereas

$$\rho(f) = x^3 + x^2 - 5x - 6. \tag{70}$$

Checking the a priori possible zeros $\pm 1, \pm 2, \pm 3, \pm 6$ of $\rho(f)$, we see that -2 is an actual zeros. Therefore $\mathrm{Gal}(f)$ is isomorphic to either D_4 or C_4. As the polynomial f turns out not to split over its stem field, we conclude that $\mathrm{Gal}(f) \simeq D_4$.

(iv) Let $f = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$. Then $\Delta(f) = 125$ is not a square, whereas

$$\rho(f) = x^3 - x^2 - 3x + 2. \tag{71}$$

Checking the a priori possible zeros $\pm 1, \pm 2$ of $\rho(f)$, we see that 2 is an actual zero. Therefore $\mathrm{Gal}(f)$ is either isomorphic to either D_4 or C_4. One of the zeros of f in $\mathbb{C}$ is given by $-\zeta_5 = -e^{2\pi i/5}$, and in fact the results of Section 4 can be used to show that

$$f = (x + \zeta_5)(x - \zeta_5^{-1})(x + \zeta_5^2)(x - \zeta_5^{-2}). \tag{72}$$

Since this polynomial splits into linear factors over the stem field $\mathbb{Q}(\zeta_5)$ of f, we see that $\mathrm{Gal}(f) \simeq C_4$.

(v) Let $f = x^4 - x^2 + 1 \in \mathbb{Q}[x]$. Then $\Delta(f) = 144 = 12^2$, whereas

$$\rho(f) = x^3 + x^2 - 4x - 4. \tag{73}$$

Checking the a priori possible zeros $\pm 1, \pm 2, \pm 4$ of $\rho(f)$, we see that $-1, -2, 2$ are actually zeros. Therefore $\mathrm{Gal}(f) \simeq V_4$.

As V_4 has two subgroups of index 2 whose intersection is trivial, Theorem IV.3.3(i) implies that the splitting field L of f (which coincides with its quartic stem field) is BIQUADRATIC; in other words, it is the compositum of two quadratic extensions. As in Example III.1.7(i), we can complete the square to see that these quadratic extensions are obtained via suitable square roots. Therefore there exist $d_1, d_2 \in \mathbb{Q}$ such that

$$L = \mathbb{Q}[x]/(f) \simeq \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}). \tag{74}$$

Let us try to find d_1 and d_2 in the particular example under consideration. As $V_4 \subset A_4$, we will unfortunately not find a quadratic subextension of L by means of the discriminant. Instead, we take a hint from the resolvent and construct expressions in the roots $\beta_1, \ldots, \beta_4$ of f that transform appropriately under the elements of its Galois group V_4. We take

$$\begin{aligned} \delta_1 &= \beta_1 + \beta_2 - \beta_3 - \beta_4, \\ \delta_2 &= \beta_1 - \beta_2 + \beta_3 - \beta_4, \\ \delta_3 &= \beta_1 - \beta_2 - \beta_3 + \beta_4. \end{aligned} \tag{75}$$

Then δ_1 is stabilized by $\langle (1\ 2)(3\ 4) \rangle$, whereas the other elements of V_4 transform it to $-\delta_1$. Similarly, the quadratic orbits of the other δ_i are also

given by $\{\pm\delta_i\}$. In light of Corollary III.2.5, it therefore stands to reason that the δ_i define quadratic extensions of $\mathbb{Q}$. However, as always it is a priori possible that some of these elements are zero.

In line with our general philosophy, we will not actually evaluate the δ_i in L; instead, we will determine their squares δ_i^2, which are fixed by the action of V_4 and therefore belong to $\mathbb{Q}$. To this end, we observe that in the notation of Proposition 2.11 we have

$$\begin{aligned}
\delta_1^2 &= \beta_1^2 + 2\beta_1\beta_2 - 2\beta_1\beta_3 - 2\beta_1\beta_4 + \beta_2^2 - 2\beta_2\beta_3 - 2\beta_2\beta_4 + \beta_3^2 + 2\beta_3\beta_4 + \beta_4^2 \\
&= \alpha_2^2 - 4\gamma_2 - 4\gamma_3, \\
\delta_2^2 &= \beta_1^2 - 2\beta_1\beta_2 + 2\beta_1\beta_3 - 2\beta_1\beta_4 + \beta_2^2 - 2\beta_2\beta_3 + 2\beta_2\beta_4 + \beta_3^2 - 2\beta_3\beta_4 + \beta_4^2 \\
&= \alpha_2^2 - 4\gamma_1 - 4\gamma_3, \\
\delta_3^2 &= \beta_1^2 - 2\beta_1\beta_2 - 2\beta_1\beta_3 + 2\beta_1\beta_4 + \beta_2^2 + 2\beta_2\beta_3 - 2\beta_2\beta_4 + \beta_3^2 - 2\beta_3\beta_4 + \beta_4^2 \\
&= \alpha_2^2 - 4\gamma_1 - 4\gamma_2.
\end{aligned} \tag{76}$$

We have $\alpha_2 = 0$ for f, and the γ_i are the zeros $-1, -2, 2$ of $\rho(f)$, so that (76) implies

$$\left\{\delta_1^2, \delta_2^2, \delta_3^2\right\} = \{12, -4, 0\}. \tag{77}$$

We mention that we cannot meaningfully order the δ_i unless (for example) an ordering of the roots of f, which we did not want to compute, is fixed. But this is irrelevant, as (not coincidentally) there is a symmetry among the three sums in (76), in that they constitute the full set of sums involving the different pairs of γ_i.

Note that we did get unlucky, in that one of the δ_i was non-zero. But not unlikely enough! We can still conclude that L contains the square roots of 3 and -1, so that this quartic field must be given by

$$L = \mathbb{Q}(\sqrt{3}, \sqrt{-1}). \tag{78}$$

This conclusion can also be obtained by explicit calculation, as the zeros of $f = x^4 - x^2 + 1$ are given by

$$\pm\frac{\sqrt{1 \pm \sqrt{-3}}}{2} = \pm\frac{\sqrt{3} \pm \sqrt{-1}}{2}. \tag{79}$$

However, equalities such as (79) can be somewhat difficult to spot, especially since they usually do not occur at all. This is another reason why the general method is usually preferable. ❀

Remark 2.13. (i) The polynomials in Example 2.12 were taken from the LMFDB [LMF24]; in all cases, they are the monic integral polynomials of smallest discriminant with the Galois group in question.

(ii) The reason that the resolvent cubic of a quartic polynomial f provides us with what we need in this section is that it involves expressions in the roots of f, namely the γ_i from (56), that are fixed when permuting their

indices by the subgroup D_4 of interest, but that get permuted among each other when applying elements of the larger group S_4. Taking the full orbit of the resulting images as in (27), we obtained a polynomial $\rho(f)$ with coefficients in the ground field that translates the question whether $\mathrm{Gal}(f)$ is contained in some subgroup conjugate to D_4 into the question whether $\rho(f)$ has a zero in the ground field K.

In Section VII.1, we will see how to generalize this method to higher degree; we will construct expressions in the roots of f that remain fixed under a given subgroup $H \subset S_n$, and by symmetrizing appropriately, we will be able to detect whether $\mathrm{Gal}(f)$ is contained in some subgroup conjugate to H by determining the zeros in K of a suitable resolvent polynomial in $K[x]$. ❁

3 Finite fields

Once we know Galois theory, the theory of finite fields reduces to a brief footnote.

Theorem 3.1. *Let K be a finite field of cardinality q, and let $L|K$ be an extension of degree n. Then L is the splitting field over K of the polynomial*

$$f = x^{q^n} - x \in K[x]. \tag{80}$$

The extension $L|K$ is Galois, and its Galois group $\mathrm{Gal}(L|K)$ is cyclic of order n, generated by the Frobenius automorphism

$$\begin{aligned} \sigma_q : L &\to L, \\ \beta &\mapsto \beta^q. \end{aligned} \tag{81}$$

Proof. This is nothing but Example III.2.8. ♡

Corollary 3.2. *Let $L|K$ be an extension of finite fields of order n with $\#K = q$. Then the subextension $M|K$ of $L|K$ are exactly the subfields of L of order q^m, where m divides $[L:K]$.*

Proof. The cyclic subgroups of $\mathrm{Gal}(L|K) = \langle \sigma_q \rangle$ are exactly the subgroups $\langle \sigma_q^d \rangle$ for a divisor d of n. Given d, the corresponding fixed field consists of the set of zeros of $x^{q^d} - x \in K[x]$ which is isomorphic to the finite field of cardinality q^d. The result is therefore a consequence of Theorem IV.1.2, which implies that any subextension $M|K$ of $L|K$ is such a fixed field. ♡

Remark 3.3. Galois' work on finite fields was published during his lifetime (1830) in a paper called *Sur la théorie des nombres* [Gal89]. It includes most important results on these extensions, though the very short paper, which runs to about ten pages, is difficult to read by modern standards; at the time, mathematics was presented in a far less systematic way, and moreover the article contains proofs of the type "Les personnes habituées à la théorie des équations le verront sans peine." ❁

4 Cyclotomic fields

This section, which can be consider as an extended example, will furnish another important family of Galois extensions. These are defined by elements of finite multiplicative order in algebraic extensions of a given ground field.

Definition 4.1. Let $L|K$ be a field extension, and let $\zeta \in L$. Then ζ is called a ROOT OF UNITY if there exists some integer $N > 0$ such that

$$\zeta^N = 1. \tag{82}$$

If ζ holds, then ζ is also called an N-TH ROOT OF UNITY. Finally, if N is the smallest integer such that (82) holds, then ζ is also called a PRIMITIVE N-TH ROOT OF UNITY. ✌

Example 4.2. If $L = \mathbb{C}$, then a primitive n-th root of unity is given by

$$\zeta_N = e^{2\pi i/N} \in L, \tag{83}$$

as follows by considering the complex argument $2\pi/N$ of ζ_N. ❀

Lemma 4.3. *Let $L|K$ be a field extension, and let $\zeta_N \in L$ be a primitive N-th root of unity. Then the following statements hold.*

(i) The N-roots of unity in L are exactly the powers of ζ_N.

(ii) If $k \in \mathbb{Z}$, then ζ_N^k is once again an N-th root of unity if and only if $\gcd(k, N) = 1$.

Proof. (i): Certainly any power ζ_N^k is again an N-th root of unity, since

$$(\zeta_N^k)^N = (\zeta_N^N)^k = 1^k = 1. \tag{84}$$

Conversely, the condition that ζ_N be a primitive root of unity amounts to stating that ζ_N is of order N as an element of the multiplicative group $\mathbb{C}^*$. Therefore the cardinality of the set of powers $\langle \zeta_N \rangle$ of ζ_N equals N.

Now any other root of unity in L is a zero of the polynomial $x^N - 1$ by definition. On the one hand, the set of zeros of this polynomial has at most N elements, yet on the other hand we just found N of them, namely the elements of the set $\langle \zeta_N \rangle$. Therefore these sets coincide, which is just another way of stating (i).

(ii): The fact that ζ_N is of order N means that there exists a group isomorphism

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} &\xrightarrow{\varphi} \langle \zeta_N \rangle \\ \overline{k} &\mapsto \zeta_N^k \end{aligned} \tag{85}$$

Since φ is an isomorphism, an element ζ_N^k generates the codomain $\langle \zeta_N \rangle$ of φ if and only if the corresponding element $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$ generates its codomain. The latter is the case if and only if $\gcd(k, N) = 1$. ♡

Roots of unity determine Galois extensions of the base field, at least under a mild separability condition.

Proposition 4.4. *Let K be a field, and let $N > 0$ be prime to the characteristic of K. Then the following statements hold.*

(i) The field extension $K(\zeta_N)|K$ is Galois.

(ii) If $\zeta \in K(\zeta_N)$ has the same minimal polynomial as ζ_N, then ζ is again a primitive root of unity.

(iii) We have $[K(\zeta_N) : K] \leq \varphi(N)$.

Proof. (i): The primitive root of unity ζ_N is in particular a zero of the polynomial $g = x^N - 1$. Since $g' = Nx^{N-1}$ is non-zero because of our assumption on N, and $g(0) = -1 \neq 0$, we see that $\gcd(g, g') = 1$. By Proposition 1.6, this implies that $x^N - 1 \in K[x]$ is separable. This means in particular that ζ_N is separable over K, so that $K(\zeta_N)|K$ is separable over K by Proposition II.2.10.

Is therefore remains to prove that $K(\zeta_N)|K$ is normal. To this end, we will apply Corollary 1.13. Let $f \in K[x]$ be the minimal polynomial of ζ_N; our goal is to show that f has all its zeros in $K[x]/(f) \simeq K(\zeta_N)$. Since ζ_N is a zero of the polynomial $x^N - 1$, we see that f divides this polynomial. As in the proof of Lemma 4.3(i), we see that $x^N - 1$ has the N distinct zeros ζ_N^k for $k = 0, \dots N - 1$. Unique factorization therefore implies that

$$x^N - 1 = \prod_{0 \leq k < N} (x - \zeta_N^k). \tag{86}$$

All zeros of $x^N - 1$ are therefore contained in $K(\zeta_N)$, and therefore the same is true for the zeros of f, which is what we wanted to show.

(ii): Since ζ_N and ζ have the same minimal polynomial, the sets of polynomial that vanish on either of these elements coincide. By considering polynomials of the form $x^m - 1$, we see that the multiplicative order of ζ coincides with that of ζ_N. This order therefore equals N, so that ζ is indeed a primitive N-th root of unity.

(iii): By Corollary III.2.5, the degree of the minimal polynomial Φ_N of ζ_N equals the length of its Galois orbit, that is, the number of elements of the form $\sigma(\zeta_N)$ for $\sigma \in \mathrm{Aut}(K(\zeta_N)\,|\,K)$. Since σ is an automorphism, Proposition I.1.5 implies that the set of polynomials in $K[x]$ that vanish in ζ_N coincides the set of polynomials that vanish in $\sigma(\zeta_N)$. Part (ii) shows that this requires $\sigma(\zeta_N)$ to be another primitive N-th root of unity, and Lemma 4.3(ii) shows that there are at most $\#(\mathbb{Z}/N\mathbb{Z})^*$ such roots, which concludes the proof. ♡

For a wonderful proof of the following theorem for the case $K = \mathbb{Q}$, which can be read without further background, we refer to [Mil22, Theorem 5.10]. There is an alternative proof using the theory of number rings, but we do not give it here, since it would lead us too far afield.

Theorem 4.5. *Let $N > 0$. Then the minimal polynomial of ζ_N over $\mathbb{Q}$ is given by*

$$\Phi_N = \prod_{\substack{0 \leq k < N \\ \gcd(k,N)=1}} (x - \zeta_N^k). \tag{87}$$

In particular, we have $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N)$.

Remark 4.6. The polynomial Φ_N is also known as the N-th CYCLOTOMIC POLYNOMIAL. It can be determined recursively over the field $\mathbb{Q}$ itself by means of the equation

$$\Phi_N = \frac{x^N - 1}{\prod_{\substack{d|N \\ d \neq N}} \Phi_d}, \tag{88}$$

for which see Exercise 9. ❁

An important corollary of Theorem 4.5 is the following.

Corollary 4.7. *Let $N > 0$. Then for any k with $0 < k < N$ such that $\gcd(k, N) = 1$ there exists a unique $\mathbb{Q}$-automorphism $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ such that*

$$\sigma_k(\zeta_N) = \zeta_N^k. \tag{89}$$

Moreover, the map

$$\begin{aligned} (\mathbb{Z}/N\mathbb{Z})^* &\to \mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q}) \\ \overline{k} &\mapsto \sigma_k \end{aligned} \tag{90}$$

is an isomorphism of groups.

Proof. Given an integer k as in the statement of the Corollary, Theorem 4.5 shows that the minimal polynomials of ζ_N and ζ_N^k coincide, since both elements are zeros of the irreducible polynomial Φ_N. The theory of simple extensions thus implies the existence of an isomorphism

$$\begin{aligned} \sigma_k : \mathbb{Q}(\zeta_N) &\to \mathbb{Q}(\zeta_N^k) \\ \zeta_N &\mapsto \zeta_N^k. \end{aligned} \tag{91}$$

Since ζ_N and ζ_N^k are both primitive by Lemma 4.3(ii), we see that either of them is a power of the other, so that both generates the field $\mathbb{Q}(\zeta_N)$. Therefore σ can be considered as an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$.

Now given k and ℓ between 0 and $N-1$ we have

$$\sigma_{k\ell}(\zeta_N) = \zeta_N^{k\ell} = (\zeta_N^k)^\ell = \sigma_k(\zeta_N)^\ell = \sigma_k(\zeta_N^\ell) = \sigma_k(\sigma_\ell(\zeta_N)) = (\sigma_k\sigma_\ell)(\zeta_N), \tag{92}$$

so that the aforementioned uniqueness implies that $\sigma_{k\ell} = \sigma_k\sigma_\ell$. Since k and ℓ were arbitrary, this shows that (90) is a homomorphism. Since Theorem 4.5 shows the second equality in the chain

$$\#(\mathbb{Z}/N\mathbb{Z})^* = \varphi(N) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}], \tag{93}$$

it suffices to show that (90) is injective. This is the case because the powers ζ_N^k for $0 < k < N$ are mutually distinct, so that the same is the case for the various images $\sigma(\zeta_N)$. ♡

Remark 4.8. (i) It is important to point out that Corollary 4.7 is indeed a corollary of Theorem 4.5, and **not** of the mere Galois statement in Proposition 4.4. Indeed, it is only Theorem 4.5 that allows us to conclude that the minimal polynomials of ζ_N and ζ_N^k for k with $0 < k \leq N$ such that $\gcd(k, N) = 1$ coincide, and thus to construct the automorphism σ_k.

(ii) Considered somewhat more informally, Theorem 4.5 provides the crucial knowledge that all primitive N-th roots of unity satisfy the same algebraic relations over $\mathbb{Q}$. Such statements are typically difficult to prove, and this particular one uses the fact that the base field equals $\mathbb{Q}$ in a crucial way; over $\mathbb{Q}(\sqrt{5})$ we have

$$\begin{aligned}\Phi_5 &= (x-\zeta_5)(x-\zeta_5^{-1})(x-\zeta_5^2)(x-\zeta_5^{-2}) \\ &= (x^2+\frac{1+\sqrt{5}}{2}x+1)(x^2+\frac{1-\sqrt{5}}{2}x+1),\end{aligned} \tag{94}$$

so that the elements $\zeta_5^{\pm 1}$ satisfy the relation $x^2+\frac{1+\sqrt{5}}{2}x+1$, which is not satisfied by $\zeta_5^{\pm 2}$. Using Theorem IV.3.3, this leads to an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}(\sqrt{5})) \simeq C_2$, whereas Corollary 4.7 implies that $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q})$ is cyclic of order 4 instead.

(iii) Similarly, since Φ_N is the minimal polynomial of ζ_N over $\mathbb{Q}$, we see that the converse of Proposition 4.4(ii) holds for $K=\mathbb{Q}$. As Part (ii) shows, it does not hold for $K=\mathbb{Q}(\zeta_5)$, as (94) implies that ζ_5 and ζ_5^2 have different minimal polynomials over K.

(iv) While we will not have $\mathrm{Gal}(K(\zeta_N)|K) \simeq (\mathbb{Z}/N\mathbb{Z})^*$ for every field K such that $\mathrm{char}(K)$ is coprime to N, as mentioned in Part (ii), the Galois group will always be abelian; see Exercise 10. ❁

5 The inverse Galois problem

The main idea behind Galois theory is that any finite normal and separable field extension gives rise to a Galois group, and that properties of this group translate to properties of the original field extension. We can try to put this situation on its head and ask whether any finite group can in fact be realized as a Galois group; after all, perhaps this would help us to think of this group and its elements in a more algebraic or geometric way. Though it has many subtle variants, the answer to the "vanilla" version of this question is positive.

Proposition 5.1. *Let G be a finite group. Then there exists a field extension $L|K$ with $\mathrm{Gal}(L|K) \simeq G$.*

Proof. Fix an embedding of G into some symmetric group S_n, for example that obtained by the action of G on itself by left multiplication, and let $L = k(x_1,\dots,x_n)$ for some field k. In Section III.3 we have already seen that S_n can be interpreted as a subgroup of $\mathrm{Aut}(L)$ via permutation of the coordinates. Therefore Theorem IV.1.2(i) implies that the extension $L|L^G$ satisfies $\mathrm{Gal}(L|L^G) = G$. ♡

Remark 5.2. Proposition 5.1 provides an answer to a version of the so-called INVERSE GALOIS PROBLEM. However, there is a more restrictive version of this problem, which ask whether given a finite group G there exists a finite Galois extension L of the field of rational numbers $\mathbb{Q}$ for which $\mathrm{Gal}(L|\mathbb{Q}) \simeq G$.

The answer to this question is still unknown. Among the finite simple groups, the Mathieu group M_{23} still stubborn resists any attempts to realize it as a Galois group over $\mathbb{Q}$. (The author of these notes once thought that he had found such a realization; then he learned more mathematics.)

To realize G as a Galois group over $\mathbb{Q}$, one would ideally want to take a realization as in the proof of Proposition 5.1 with $k = \mathbb{Q}$ and then "specialize" the variables involved appropriately to obtain a realization over $\mathbb{Q}$ itself. The general theory of "thin sets" shows that this is indeed possible provided that $\mathbb{Q}(x_1, \ldots, x_n)^G$ comes from a geometric object that admits defining equations over $\mathbb{Q}$. However, despite appearances to the contrary, this is in general quite difficult, as $\mathbb{Q}(x_1, \ldots, x_n)^G$ might contain superfluous constant functions that give an obstruction to obtaining a sensible geometric object over $\mathbb{Q}$. For more information on this relentlessly subtle topic, which is related to that in Section VI.5, one can consult the advanced lecture notes [Ser92]. ❁

6 Exercises for Chapter V

Exercise 1. Let $G \subset S_4$ be an intransitive subgroup. Show that exactly one of the following statements holds true.

(i) G is conjugate a subgroups of S_3 acting on $\{1, 2, 3\}$.

(ii) G is conjugate to $\langle (1\ 2)(3\ 4) \rangle \simeq C_2$.

(iii) G is conjugate to $\langle (1\ 2), (3\ 4) \rangle \simeq V_4$.

Exercise 2. Let $G \subset S_5$ be an intransitive subgroup. Show that exactly one of the following statements holds true.

(i) G is conjugate to a subgroup of S_4 acting on $\{1, 2, 3, 4\}$.

(ii) G is conjugate to a product of transitive subgroups of S_3 (acting on $\{1, 2, 3\}$) and $\langle (4, 5) \rangle$.

(iii) G is conjugate to $\langle (1\ 2\ 3), (2\ 3)(4\ 5) \rangle$.

Exercise 3. Let $G \subset S_n$ be a non-trivial normal subgroup. Show that G is transitive.

Exercise 4. Consider the polynomials

$$D = \prod_{1 \le i < j \le n} (x_i - x_j)^2, \quad B = \prod_{1 \le i < j \le n} (x_i + x_j), \quad \text{and} \quad C = (B^2 - D)/4$$

in $\mathbb{Z}[x]$. Let K be a field of characteristic 2, let $f \in K[x]$ be a separable polynomial with zeros $\beta_1, \cdots, \beta_n$, and let b (respectively c) be the element of L obtained from B (respectively C) by substituting β_i for x_i for all i between 1 and n.

(i) Show that b and c are in fact elements of K.

(ii) Show that $\mathrm{Gal}(f) \subset A_n$ if and only if the polynomial $x^2 + bx + c$ in $K[x]$ has a zero in K.

Exercise 5. Let K be a field, let n and m be positive integers, and consider polynomials

$$f = \alpha_0 + \ldots + \alpha_n x^n \quad \text{and}$$
$$g = \beta_0 + \ldots + \beta_m x^m.$$

Define the SYLVESTER MATRIX $S(f,g) \in M_{m+n,m+n}(K)$ associated to f and g to be the matrix whose first m rows are the m rightward shifts (including the trivial one) of

$$(\alpha_0, \ldots, \alpha_n, 0, \ldots, 0)$$

and whose subsequent n rows are the n rightward shifts (including the trivial one) of

$$(\beta_0, \ldots, \beta_m, 0, \ldots, 0).$$

(i) Show that $s(f,g) = \det(S(f,g))$ satisfies the properties described in Proposition 1.10, except that no scalar is involved in Part (iii).

(ii) Show that $s(f,g)$ is the determinant of the matrix representation of the K-linear map

$$K[x]_{m-1} \times K[x]_{n-1} \to K[x]_{m+n-1}$$
$$(a,b) \mapsto af + bg$$

with respect to the standard basis $(1, t, \ldots)$ of $P_n(K)$.

Exercise 6. In the situation of Theorem 2.9, show that if $\mathrm{Gal}(f) \simeq D_4$, then f has exactly two roots over its stem field. (Hint: Show that the stabilizer of any root of f also stabilizes exactly one of its other roots.)

Exercise 7. Show that the groups H_1, H_2, and H_3 from Section 2 are the inverse images of the subgroups of order 2 of S_4/V_4 under the canonical projection homomorphism $S_4 \to S_4/V_4$.

Exercise 8. Prove Equation (72).

Exercise 9. Prove Equation (88).

Exercise 10. Let K be an arbitrary field, and let $N > 0$.

(i) Show that there exists a primitive N-th root of unity ζ_N in $\overline{K}$.

(ii) Show that $K(\zeta_N)|K$ is a finite Galois extension if and only N is coprime to the characteristic of K.

(iii) Show that if N is coprime to the characteristic of K, then $\mathrm{Gal}(K(\zeta_N)|K)$ is abelian of cardinality dividing $\varphi(N)$.

Exercise 11. For each of the following pairs K and f, determine the Galois group of the polynomial $f \in K[x]$. You may use that f is separable and irreducible in all cases.

(i) $K = \mathbb{Q}$, $f = x^3 - x^2 + 1$.

(ii) $K = \mathbb{Q}$, $f = x^3 - 3x - 1$.

(iii) $K = \mathbb{Q}$, $f = x^4 - x^3 + 2x + 1$.

(iv) $K = \mathbb{Q}$, $f = x^4 - x^3 + 2x + 1$.

(v) $K = \mathbb{Q}$, $f = x^4 + 1$.

(vi) $K = \mathbb{Q}$, $f = x^4 - x^3 - 4x^2 + 4x + 1$.

(vii) $K = \mathbb{Q}$, $f = x^4 - x^3 - 3x + 4$.

(viii) $K = \mathbb{Q}$, $f = x^4 + x^2 - x + 1$.

(ix) $K = \mathbb{F}_3(t)$, $f = x^4 - x - 1$.

(x) $K = \mathbb{F}_3(t)$, $f = x^4 + x^2 + t$.

(xi) $K = \mathbb{F}_3(t)$, $f = x^4 + tx^2 + 1$.

(xii) $K = \mathbb{F}_3(t)$, $f = x^4 + x^3 + tx^2 + x + 1$.

Summary and main notions of the chapter

This time, the motivating Question (i) in the introduction to this chapter has a somewhat longer answer.

- If $f \in K[x]$ is a separable irreducible cubic polynomial over a field K with $\mathrm{char}(K) \neq 2$, then Theorem 1.15 shows that the Galois group of f can be determined by using the discriminant $\Delta(f)$ from Definition 1.2.
- If $f \in K[x]$ is a separable irreducible quartic polynomial over a field K with $\mathrm{char}(K) \neq 2$, then Theorem 2.9 shows that the Galois group of f can be determined by using the discriminant $\Delta(f)$ along with the resolvent cubic $\rho(f)$ from Definition 2.6.
- The Galois groups of some special families allow a uniform description, such as those of finite fields (Theorem 3.1) and cyclotomic fields (Theorem 4.5) are also known.

The key skills to take away from this chapter are the following:

- You are able explicitly to determine the Galois group of a separable irreducible cubic polynomial $f \in K[x]$, as described above. Moreover, you know the explicit formula $\Delta(f) = -4a^3 - 27b^2$ for cubic polynomials f of the form $x^3 + ax + b$. For more general cubic polynomials, you can compute the discriminant by means of the resultant, as described in Proposition 1.12 and applied in Exercise 1.14.
- You are able explicitly to determine the Galois group of a separable irreducible quartic polynomial $f \in K[x]$, as described above. Moreover, you know how to determine the discriminant $\Delta(f)$ of such a polynomial by means of Proposition 1.12, and you are aware of Proposition 2.11, which describes the resolvent cubic of a given quartic polynomial.

– You know how to describe the Frobenius automorphism generating the Galois group of an extension of finite fields (Theorem 3.1).

– You can describe the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_N)|\mathbb{Q}$ as in Corollary 4.7.

Chapter VI

Applications of Galois theory

This chapter tells some of the stories about how Galois theory, as well as general field theory, resolved questions that were around for millennia before the introduction of these concepts allowed mathematicians to settle them once and for all. Elaborating upon them is often an enjoyable theme for a bachelor, master, or PhD thesis.

1 Big trouble in ancient Greece

The theory of fields can be used to resolve many questions relating to the classical theme of constructions with ruler and compass. This is a problem that was first explored by the ancient Greeks. Suppose that one is given the real plane along with the two points $(0,0)$ and $(1,0)$, a straightedge, and a compass. Then we can start drawing geometric figures, using the following rules:

(C1) We may only use the straightedge to create lines that pass through pairs of points that we have already constructed.

(C2) We may only use the compass to create lines whose base is one the points that we have already constructed, and whose radius is a distance between two of these points.

(C3) We may only create new points as intersections of the lines and circles created in Parts (i) and (ii).

This leads to the following logical question: What kind of points and what line segments can we obtain by means of these constructions?

Typical examples that interested the ancient Greeks were the following:

(i) (Squaring the circle) Consider a circle C with radius 1. Can we construct a square with the same area as C?

(ii) (Doubling the cube) Can we construct a cube with volume 2?

(iii) (Trisecting the angle) Let a point $P = (\cos(\vartheta), \sin(\vartheta))$ on the unit circle be given in addition. Can we construct the point $Q = (\cos(\vartheta/3), \sin(\vartheta/3))$ whose angle with the (positive) x-axis is a third of that of P?

(iv) (Constructing n-gons) Let $n > 2$. Can we construct a regular n-gon?

This question is far from easy. At some point, the realization began to dawn that most of them could be impossible to solve. Still, the Greeks kept trying, because… well, for one, why would one not be able not find all numbers this way? The discovery (or should that be the construction?) of the real numbers is far from obvious, and it took millennia to arrive at the current definition, according to which most real numbers are completely inscrutable; the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ inside $\mathbb{C}$ is tiny, being a merely countable subset of the uncountable set $\mathbb{C}$, and working with real numbers leads to ridiculous results like the Banach–Tarski paradox, which for the Greeks would have been a strong argument against using them.

In fact some ancient mathematicians did find ways to solve the problems above; but these involve intricate geometric constructions that need other tools than ruler and compass. One of them employs a marked rotatable ruler. The use of this method, called νεῦσις, was frowned upon by purists such as by Euclid. Still, Archimedes (287–212 BCE) used them to accomplish the trisection of the angle and the doubling of the cube. According to one account of his death, Archimedes refused to stop working on a problem involving circles ("μὴ μου τοὺς κύκλους τάραττε") when summoned by a Roman soldier to appear before the victor of the siege of Syracuse and was then killed by the soldier. Such were the customs of the time.

But we digress. Using the theory of fields, one can give full answers to these old questions, and show that most constructions above are indeed impossible. Indeed, by carefully analyzing the possible constructions (a good theme for a bachelor's thesis), one can show that if K is a field generated by the coordinates of points obtained using a finite number of iterations of the permitted constructions, then $[K : \mathbb{Q}]$ is a power of 2. Squaring the circle is therefore impossible, because it amounts to constructing a line segment of length $\sqrt{\pi}$. But then we would have $\sqrt{\pi} \in K$, and therefore $\pi \in K$, which is impossible; we would obtain that π is algebraic, whereas it is in fact transcendental.

Similarly, we cannot trisect the cube in this way, as it requires is to construct a line segment of length $\sqrt[3]{2}$, so that $\sqrt[3]{2} \in K$. Now this time $\sqrt[3]{2}$ is algebraic, but we would then obtain $\mathbb{Q}(\sqrt[3]{2}) \subset K$, so that

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]. \tag{1}$$

by the tower law. However, $\sqrt[3]{2}$ is a zero of the irreducible polynomial $f = x^3 - 2$, which is therefore the minimal polynomial of $\sqrt[3]{2}$. The theory of simple extensions then implies that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(f) = 3$, so that $[K : \mathbb{Q}]$ is divisible by 3 in light of (1), which is nonsense. A similar argument shows the impossibility of trisecting a general angle ϑ.

As for the constructibility of n-gons, in 1796 Gauß showed that it is possible to construct a regular 17-gon, which immediately made him famous, and in the

Disquisitiones Arithmeticae, he showed that if $n > 2$, then a regular n-gon can be constructed if

$$n = 2^k F_1 \cdots F_r \tag{2}$$

where $k, r \geq 0$ and where the F_i are FERMAT PRIMES, that is, prime numbers of the form

$$F_i = 2^{2^{m_i}} + 1 \tag{3}$$

for some $m_i \geq 0$. The only Fermat primes known so far are

$$3,\ 5,\ 17,\ 257,\ 65537, \tag{4}$$

and it is conjectured that there are no more. Gauß also stated that if, conversely, a regular n-gon exists, then n is of the form (2), but he did not prove this; this was accomplished by Pierre Wantzel (1814–1848) in 1837. The construction of the 65537-gon was first achieved in 1894 by Johann Hermes (1846–1912) in a work of 200 pages. He was employed at a Gymnasium in Lingen at the time. Later he was appointed director of a Gymnasium in Osnabrück and concluded his inaugural lecture with the apt words: "Geduld ist die Pforte der Freude".[1]

The constructibility of the regular n-gon by means of νεῦσις was studied by Arthur Baragar in [Bar]. As νεῦσις turns out only to create successive field extensions of degree at most 6, there again exist n-gons that cannot be constructed by means of it, the first of which is the 23-gon. This analysis should be an enjoyable topic for a master's thesis.

As a final aside, it should be mentioned that Archimedes also investigated what happens if we just keep constructing new extensions and pass to the limit, adding ever smaller line segments; this leads to his *method of exhaustion*, which was a precursor of calculus and analysis. Once again, this was broadly thought to be unacceptable, and only further developed millennia later. It may seem ridiculous that an old culture was unable to embrace change, even highly necessary change; but considering the society and times in which we live, it would be better in this regard to keep our mouth wisely shut.

2 Solvability by radicals

From high school, you will remember that the solutions of a quadratic equation

$$ax^2 + bx + c = 0 \tag{5}$$

are given by

$$z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}. \tag{6}$$

To determine these zeros, all that is need are the usual field operations (addition, subtraction, multiplication and division) along with the extraction of square roots. The case of a cubic equation

$$ax^3 + bx^2 + cx + d = 0 \tag{7}$$

[1] See https://de.wikipedia.org/wiki/Johann_Gustav_Hermes [Accessed 16 May 2024]

is more complicated, and writing down a formula for the zeros becomes quite complicated. This is easier for the simpler standard form

$$x^3 + 3px + q = 0 \tag{8}$$

which is obtained from (7) by means of a scaling followed by a translation in the x-coordinate.

Solving (8) became something of a prestige project in Renaissance Italy, with reputations and large financial stakes on the line; competitions between mathematicians would often lead to the loss of financial income or university positions. Consequently, whatever results that were obtained were often closely guarded and shared only in rare cases, which is not very conducive to a healthy scientific climate. The first solution of (8) was due to Scipione del Ferro (1465–1526), but under certain hypotheses on the signs of p and q, essentially because of his unfamiliarity with negative numbers. He passed on his results to his student Antonio Fior only shortly before dying. Niccolò Tartaglia (1500–1557) also developed a method, which he shared with Girolamo Cardano (1501–1576) under the condition that the latter would not reveal his results. Cardano later discovered that del Ferro had already developed a method quite some time before Tartaglia, and published this method (with proper attribution to del Ferro) in his book *Ars Magna* of 1545. As a result, Tartaglia challenged Cardano, who refused; instead, the gauntlet was taken up by Cardano's student Lodovico Ferrari (1522–1565) who won the competition, to Tartaglia's ruin.[2]

Oh, and what about the solutions to (8)? These are given by

$$z_1, z_2, z_3 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{9}$$

It may seem rather astounding that del Ferro should have been able to solve (8) without even accepting negative numbers, but that is only the case with the benefit of hindsight. There were conceptual and philosophical objections to them, and while modern mathematics no longer considers these to be relevant, the solution (9) raises questions in itself. Why are there in fact only three solutions? After all, one needs to make a choose cube roots two times, which would at first sight lead to nine solutions. What gives? Furthermore, even if all solutions of (8) are real, then one may still obtain square roots of negative and/or complex numbers in (9). It is anything but trivial to define the exact algebraic structure in which the answers lie, or to see when a solution in the real or rational numbers exists, and much of the theory of fields was developed in order to be able to provide sensible answers to such questions. In fact finding out why (9) gives the solutions to (8), and stating exactly which quadratic and cube roots have to be taken, remains an interesting theme for a bachelor's thesis.

One of its main original motivations was another one, however. As before, the solutions (9) only involve field operations and "radicals", that is, general n-th roots. This continues to be true for quartic equations, but at this point, the mathematical collective ran into a steel wall; no-one managed to find a formula

[2] See https://en.wikipedia.org/wiki/Cubic_equation#History [Accessed 16 May 2024]

for centuries on end. This turned out not to be due to any failing of creativity on the part of mathematicians; in 1799, Paolo Ruffini (1765–1822) was the first to claim a proof of the impossibility of solving the general equation of degree 5 by means of radicals. Not only did this incur him the ire of quite a few of his colleagues, but his proof was flawed; it took until 1824 for Nils Henrik Abel (1802–1829) to give a correct proof.

Of course, there is no reason why one should be able to obtain all algebraic numbers by means of radicals... but then again, there is also no obvious reason why one should not. Moreover, some quintic equations are solvable by radicals, such as

$$x^5 - 2 = 0. \tag{10}$$

The same is the case for the minimal polynomial of $\alpha = 1 + \sqrt[5]{2} + \sqrt[5]{4}$, which defines the same field extension as $\sqrt[5]{2}$ but which instead satisfies the equation

$$x^5 - 5x^4 + 10x^3 - 20x^2 + 15x - 7 = 0, \tag{11}$$

for which it is far from clear that is admits a solution by radicals. What is therefore the intrinsic property that can make an equation solvable or unsolvable in this way? This was the question that Abel had not quite yet answered, and that Galois' work would solve. We will briefly sketch his results in modern language.

From radicals to solvability

Suppose first that $\alpha \in \mathbb{C}$ is an algebraic number that can be obtained by means of radicals. We can then ask what the field $\mathbb{Q}(\alpha) \subset \mathbb{C}$ looks like. By construction, α is obtained by starting with elements of $\mathbb{Q}$ and then repeatedly applying addition, subtraction, multiplication and division, as well as root extraction. The final one of these operations may lead to a proper field extension. More precisely, this argument shows that α is an element of the final field in a chain

$$\mathbb{Q} \subset \mathbb{Q}(\beta_1) \subset \mathbb{Q}(\beta_1, \beta_2) \subset \ldots \subset \mathbb{Q}(\beta_1, \ldots, \beta_n), \tag{12}$$

where for $1 \leq i \leq N$ we have that

$$\beta_i^{e_i} = \gamma_i \in \mathbb{Q}(\beta_1, \ldots, \beta_{i-1}). \tag{13}$$

It turns out that the existence of the chain (12) has consequences for the Galois group of the minimal polynomial f of α. To see this, let us take N to be the least common multiple of the e_i in (13). Section V.4 shows that the extension

$$K = \mathbb{Q}(\zeta_N) \tag{14}$$

of $\mathbb{Q}$ is Galois with abelian Galois group. Now since ζ_N belongs to K, the same is the case for the roots of unity ζ_{n_i}. If we now adjoin a single zero β_i of the polynomial $g_i = x^{e_i} - \gamma_i$, as in (13), we in fact immediately obtain all the others, which are $\zeta_{n_i}^k \beta_i$ for $1 \leq k \leq n_i - 1$. Therefore the field L_i obtained by adjoining β_i is a splitting field over the smaller field L_{i-1}. This leads to the chain of field extensions

$$\mathbb{Q} \subset K =: L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n \tag{15}$$

for which $\alpha \in L_n$. Now the splitting field $L_i \,|\, L_{i-1}$ is normal by Theorem I.1.6, and it is separable by Proposition II.1.4. It is therefore finite Galois.

Moreover, the Galois group $\mathrm{Gal}(L_i \,|\, L_{i-1})$ is abelian. Indeed, any automorphism σ in $\mathrm{Aut}(L_i \,|\, L_{i-1})$ is determined by where it sends the generator β_i. Since this element is a zero of $g_i = x^{n_i} - \gamma_i \in L_{i-1}[x]$, Proposition I.1.5 shows that σ is of the form

$$\begin{aligned} \sigma_k : L_i &\to L_i \\ \beta_i &\mapsto \zeta_{n_i}^k \beta_i \end{aligned} \tag{16}$$

for some k with $1 \le k \le n_i$. Now since $\zeta_{n_i} \in K \subset L_{i-1}$, we see that if ℓ is another integer with $1 \le \ell \le n_i$, we have that

$$\begin{aligned} (\sigma_k \circ \sigma_\ell)(\beta_i) &= \sigma_k(\sigma_\ell(\beta_i)) = \sigma_k(\zeta_{n_i}^\ell \beta_i) = \sigma_k(\zeta_{n_i})^\ell \sigma_k(\beta_i) = \zeta_{n_i}^\ell \zeta_{n_i}^k \beta_i = \zeta_{n_i}^{\ell+k} \beta_i \\ &= \zeta_{n_i}^{k+\ell} \beta_i = \zeta_{n_i}^k \zeta_{n_i}^\ell \beta_i = \sigma_\ell(\zeta_{n_i})^k \sigma_\ell(\beta_i) = \sigma_\ell(\zeta_{n_i}^k \beta_i) = \sigma_\ell(\sigma_k(\beta_i)) \\ &= (\sigma_\ell \circ \sigma_k)(\beta_i). \end{aligned} \tag{17}$$

Since β_i generates L_i over L_{i-1}, this shows that $\sigma_k \circ \sigma_\ell = \sigma_\ell \circ \sigma_k$, and since k and ℓ were arbitrary, we conclude that $\mathrm{Aut}(L_i \,|\, L_{i-1})$ is indeed abelian. (In fact this group is cyclic, but that is not crucial for our argumentation.)

Theorem IV.2.3 shows that the Galois properties of the extensions $K \,|\, \mathbb{Q}$ and $L_i \,|\, L_{i-1}$ that we just described translate into the following statement on the Galois group $G = \mathrm{Gal}(L_n \,|\, \mathbb{Q})$: There exists a descending chain of subgroups

$$G =: H_{-1} \supset H_0 \supset H_1 \supset \ldots \supset H_{n-1} \supset H_n = \{e\} \tag{18}$$

with the property that H_i is normal in H_{i-1} with abelian quotient H_{i-1}/H_i for $i = 0, \ldots n$. A finite group G with this property is called SOLVABLE.

It can be shown that every quotient of a solvable finite group is again solvable. This has important consequences for the minimal polynomial $f \in \mathbb{Q}[x]$ of an element $\alpha \in \mathbb{C}$ that can be constructed by means of radicals; as $\alpha \in L$, the splitting field of f is contained in the field L, so that its Galois group (which is by definition the Galois group of f) is a quotient of G by Theorem IV.2.3. The Galois group of f is therefore solvable.

While all subgroups of S_n are solvable for $n \le 4$, it can be shown that if $n \ge 5$, neither of the groups A_n and S_n is solvable. Therefore in particular the zeros of a quintic polynomial with Galois group S_5, such as

$$x^5 - x - 1 \in \mathbb{Q}[x], \tag{19}$$

cannot be constructed by means of radicals. In fact, since "most" splitting fields of irreducible polynomials of degree $n \ge 5$ have Galois group S_n, we see that "most" algebraic numbers of degree $n \ge 5$ cannot be constructed by means of radicals.

From solvability to radicals

The results from the previous section were claimed in some form by Ruffini, though his proof was less profound (and incorrect). However, Galois' methods show even more: They also imply that if the Galois group of the minimal

polynomial $f \in \mathbb{Q}[x]$ of an algebraic element $\alpha \in \mathbb{C}$ is solvable, then in fact α can be constructed by means of radicals. To this end, we basically invert the argument above. Let L be the splitting field of f over $\mathbb{Q}$. Since $G = \mathrm{Gal}(L|\mathbb{Q})$ is solvable by assumption, there exists a descending chain

$$G =: H_0 \supset H_1 \supset \ldots \supset H_{n-1} \supset H_n = \{e\} \tag{20}$$

with the property that H_i is normal in H_{i-1} with abelian quotient H_{i-1}/H_i for $i = 1, \ldots, n$. Via Theorem IV.2.3, this translates to a chain of field extensions

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n = L \tag{21}$$

such that $L_i|L_{i-1}$ is a Galois extension with abelian Galois group for $i = 1, \ldots, n$. Since all subgroups of abelian groups are normal, we can refine further if necessary to assume that none of the extensions $L_i|L_{i-1}$ admits a proper subextension; this implies in particular that these extensions are abelian with cyclic Galois group.

We now take N to be the least common multiple of the degrees $n_i = [L_i : L_{i-1}]$, and we let $K = \mathbb{Q}(\zeta_N)$. Example IV.3.2 shows that we can make sense of the new chain of extensions

$$\mathbb{Q} \subset K = L_0K \subset L_1K \subset L_2K \subset \ldots \subset L_nK \tag{22}$$

As ζ_N is a zero of the polynomial $x^N - 1 \in \mathbb{Q}[x]$, the extension $K = \mathbb{Q}(\zeta_N)$ can indeed be constructed by taking radicals. For $1 \leq i \leq n$, Theorem IV.3.3 shows that the Galois group of the extension

$$L_iK|L_{i-1}K = L_i(L_{i-1}K)|(L_{i-1}K) \tag{23}$$

can be identified with a subgroup of the abelian group $\mathrm{Gal}(L_i|L_{i-1}K)$. Since $L_{i-1}K$ contains the N-root of unity ζ_N, a (somewhat anachronous) result by Kummer, whose cohomological proof is explored in Section VII.3, states that there exists some $\beta_i \in L_i$ such that

$$L_i = L_{i-1}(\beta_i) \quad \text{and} \quad \beta_i^{n_i} \in L_{i-1}. \tag{24}$$

We therefore see that every step in the chain can be constructed by means of radicals. Since $\alpha \in L_n \subset L_nK$, we see that α can be constructed by means of radicals as well, which is what we wanted to show.

The results on solvability by radicals that were sketched above are quite literally the raison d'être of Galois theory. Contemporary mathematics does not put great emphasis on the problem of solvability; it was exactly the theory of fields that has taught us that algebraic numbers with more general defining polynomials can be grasped equally well conceptually as algebraic numbers that are obtained by repeated radical extraction. Since Newton's method allows us to find good numerical (real or complex) approximations for these more general algebraic numbers as well, there in many respects no reason to restrict oneself to solvable algebraic extensions.

However, the idea of Galois theory has proven itself to be so profound and useful that it continues to play an essential role in areas far beyond it. The upcoming sections describe the role that it plays in some contemporary mathematical problems and theories.

How Galois described his result

But before we dive into these newer themes, we quickly consider Galois' own version of his results in his *Mémoire* [Gal89], which is as follows:

"Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement."

In modern terms, Galois proved that the roots of an irreducible polynomial $f \in \mathbb{Q}[x]$ of **prime** degree has the property that its roots can be described by means of radicals if and only if the splitting L of f is generated by any two roots of f (instead requiring the adjunction of more roots). The modern formulation in terms of solvable groups is so different from this statement that, somewhat amusingly, at some point a question was asked on MathOverflow around the existence of exactly such a result, which then turned out to have been solved by Galois almost two hundred years ago; see [Mil22, Aside 5.35].

3 Class field theory

In Section 4 we already considered the CYCLOTOMIC FIELD

$$K = \mathbb{Q}(\zeta_N), \tag{25}$$

which is a Galois extension of $\mathbb{Q}$ with abelian Galois group. In fact any extension of $\mathbb{Q}$ with abelian Galois group is contained in one of the fields $\mathbb{Q}(\zeta_N)$; this surprising result is known as the KRONECKER–WEBER THEOREM. It is a special case of CLASS FIELD THEORY, which is the study of the abelian extension of a given number theory. This constellation of results was brought to completion by Teiji Takagi (1875–1960) during World War I. The isolation of Japan from the rest of the world at the time was ironically to Takagi's advantage, as the resulting independence led him to prove the crucial existence results that were the capstone of this theory without being led astray by false starts.[3] Emil Artin, whom we already met in Remark IV.1.4, provided the formalism that is still used in contemporary presentations of class field theory, especially the so-called ARTIN RECIPROCITY MAP.

To get an inkling of what class field theory is about, one can start with a logical question: Given an abelian Galois extension L of $\mathbb{Q}$, how do we determine an integer N such that L embeds into $\mathbb{Q}(\zeta_N)$? There turns out to be a smallest such integer, and it is called the CONDUCTOR of the extension $L|\mathbb{Q}$. Calculating this number is a local computation of the kind further described in Section 4; suffice to say that it involves the RAMIFICATION of primes in the ring of integers $\mathbb{Z}_L$ of the field extension $L|\mathbb{Q}$. In particular, if L is defined by a monic polynomial $f \in \mathbb{Z}[x]$, then the conductor can only contain primes p such that f modulo p is separable. Such primes can be determined by computing the DISCRIMINANT of f, as introduced in Definition V.1.2.

Once the conductor N of L is known, we can compute a special automorphism σ_p of L for every prime p that does not divide N. This automorphism of L

[3] See https://en.wikipedia.org/wiki/Teiji_Takagi#Biography [Accessed 16 May 2024]

is called the Frobenius automorphism of L, and it can be understood most concretely as the restriction of the map

$$\begin{aligned} \sigma_p : \mathbb{Q}(\zeta_N) &\to \mathbb{Q}(\zeta_N) \\ \zeta_N &\mapsto \zeta_N^p \end{aligned} \tag{26}$$

to L. Modulo any prime of L, the isomorphism σ_p induces the Frobenius automorphism of the corresponding finite field. The Artin reciprocity map gives information on the various combination of the maps σ_p in terms of the arithmetic of the ring of integers $\mathbb{Z}_L$, and in particular its existence implies that σ_p is trivial if and only of p splits as a product of distinct prime ideals of $\mathbb{Z}_L$ with residue field $\mathbb{F}_p$.

This result is not as abstruse as it may seem at first sight. For the cyclotomic extension $L = \mathbb{Q}(i)$ of conductor $N = 4$, the automorphism σ_p is well-defined provided that p is odd, and its description (26) shows that σ_p is trivial if and only if $p \equiv 1 \bmod 4$. On the other hand, the existence of the Artin reciprocity map along with the fact that the ring of integers $\mathbb{Z}[i]$ is a principal ideal domain imply that this happens if and only if $p = \pi_1\pi_2$ in $\mathbb{Z}[i]$ with $\mathrm{Nm}(\pi_1) = p = \mathrm{Nm}(\pi_2)$, which is the case if and only of p is a sum of two squares. We thus recover the classical result that an odd prime can be written as a sum of two squares if and only if it is congruent to 1 modulo 4.

For more general quadratic fields $\mathbb{Q}(\sqrt{p})$ with p odd, the special expression

$$\sqrt{\pm p} = \sum_{n=0}^{p-1} \zeta_p^{n^2}, \tag{27}$$

(which is an example of a so-called Gauß sum) shows that $\mathbb{Q}(\sqrt{\pm p})$ embeds into $\mathbb{Q}(\zeta_p)$, and therefore that $\mathbb{Q}(\sqrt{p})$ embeds into $\mathbb{Q}(i, \zeta_p) \subset \mathbb{Q}(\zeta_{4p})$. This time the description (26) implies that given another odd prime q, the automorphism σ_q only depends on q modulo $4p$. The existence of the Artin reciprocity map then implies that the splitting behavior of q in the ring of integers of $\mathbb{Q}(\sqrt{p})$, and therefore the property whether q is a square modulo p or not, depends only on q modulo $4p$. This is one of the many equivalent ways that the quadratic reciprocity law can be phrased, and perhaps the most insightful of them all.

These are not the only elegant results that can be found using class field theory; the rabbit hole goes far deeper, and leads to deep arithmetic results on the splitting of primes, and therefore on the resolution of algebraic equations in finite fields. Moreover, it was the context of class field theory that Nikolai Chebotaryov (1894–1947) proved the amazing density results that we shall study in Section VII.2.

Chebotaryov's result is one of the reasons why the knowledge of the Galois group of a field extension is interesting; in a nutshell, it states that any ramification behavior that is compatible with the Galois group of a polynomial will occur for its reduction at some prime, and this is often highly relevant when solving Diophantine problems, as we saw by studying the ramification behavior of primes in the fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{\pm p})$ above. For example, it can be shown that because the polynomial

$$f = x^4 - x^2 + 1 \in \mathbb{Q}[x] \tag{28}$$

has Galois group V_4 (which does not contain any 4-cycle), there is no prime p for which f modulo p is again irreducible, whereas on the other hand there are infinitely many primes p for which the polynomial

$$f = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x] \tag{29}$$

with Galois group C_4 (which is generated by a 4-cycle), is again irreducible; in fact, this is the case for half of the primes, when measured appropriately.

Another important corollary of Chebotaryov's result is Dirichlet's result on the equidistribution of primes modulo N, which states that given $N > 0$ and a residue class $\overline{k} \in (\mathbb{Z}/N\mathbb{Z})^*$, there exist infinitely many prime numbers p such that $p = \overline{k}$ modulo N, and that moreover (again, appropriately measured) the density of such primes equals $1/\varphi(N)$. While we do not go into the details in these notes, this topic offers many interesting themes for a master thesis.

4 Conductors and L-functions

Conductors and ramification are not merely important in class field theory, but they also play a role in the study of algebraic varieties, and in particular for ALGEBRAIC CURVES over $\mathbb{Q}$, i.e. those curves that admit a polynomial description

$$X : f(x, y) = 0 \tag{30}$$

with $f \in \mathbb{Q}[x, y]$. To such a curve, one can again associate a conductor

$$N = \prod p^{e_p}, \tag{31}$$

where given a prime p the CONDUCTOR EXPONENT e_p of X at p measure how bad the singularities of the curve (or rather of its so-called JACOBIAN) are modulo p.

The computation of e_p for those finitely many primes for which is it strictly greater than zero involves the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ is the p-ADIC COMPLETION of $\mathbb{Q}$ at p; it can be seen as a local version of $\mathbb{Q}$ whose arithmetic reflects the behavior of the various algebraic extensions of $\mathbb{Q}$ over the prime p of $\mathbb{Z}$, and in fact $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ can be considered as a subgroup of the "absolute" Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$.

To obtain e_p, one studies a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ on a certain vector space V, the TATE MODULE of X, whose elements can be considered as (limits of) algebraic coordinates on an algebraic version of the tangent space of the Jacobian of X. In a sense, one provides $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ with a descending series H_i of its subgroups, called the RAMIFICATION GROUPS, that reflect ever more ramified behavior at the prime p, after which one measures how deep along this series one has to go to obtain a trivial action of H_i on V.

Questions such as these are at the heart of the work of Prof. Bouw and Prof. Wewers at the Institute of Algebra and Number Theory, and have led to multiple PhD thesis by various authors on these topics. The reason to be interested comes from the LANGLANDS PROGRAM, which is a vast scheme of conjectures and results around MODULARITY of algebraic varieties. This program can be seen as

a vast generalization of the proof found by Andrew Wiles and his co-authors for Fermat's Last Theorem. Said proof hinges on showing all algebraic curves over $\mathbb{Q}$ of a special kind (so-called ELLIPTIC CURVES) can be described by means of an analytic object called a MODULAR FORM, and the Langlands program generalizes to more general algebraic varieties.

In the context of the Langlands program, the importance of the calculation of conductor exponents stems from the fact that they indicate where to look for a modular form corresponding to a given algebraic curve. The conductor itself plays a role in the functional equation for the L-series associated to these analytic objects. Besides providing conductor exponents, the methods of Bouw and Wewers also determine the local factors of these L-series, which reflect the arithmetic behavior of the variety modulo a given prime p. Piecing these factors together, one obtains an analytic expression with a functional equation that in turn governs much of the arithmetic properties of the algebraic curve X, and that is expected to admit a description in terms of a suitable modular form.

5 Galois descent

We already alluded the role of cohomological methods when describing the proof of Kummer's theorem in Section 2. They also play a role when studying the arithmetic of complex algebraic curves, i.e. those algebraic curves that admit a polynomial equation

$$X : f(x, y) = 0 \tag{32}$$

with $f \in \mathbb{C}[x, y]$. It is often important to know when such a curve admits a defining equation whose coefficients belong to a small field.

The optimal result in this regard occurs when the coefficients of f can be chosen to belong to the smallest subfield $\mathbb{Q}$ of $\mathbb{C}$, as was the case in the previous section. A generalization of Theorem III.2.3 shows that this happens if and only if the coefficients of $f \in \mathbb{C}[x]$ are all invariant under $\mathrm{Aut}(\mathbb{C}|\mathbb{Q})$. Galois theory then provides a full characterization of when X admits a defining equation over $\mathbb{Q}$: We need that

$$\sigma(X) = X, \tag{33}$$

for every $\sigma \in \mathrm{Gal}(\mathbb{C}|\mathbb{Q})$, where the GALOIS CONJUGATE $\sigma(X)$ is defined to be the algebraic curve obtained by applying σ to the coefficients of f.

While this solves our question, the condition (33) is satisfied if and only if the polynomial f that describes X was already in $\mathbb{Q}[x]$. But of course this makes the problem of finding a defining equation over $\mathbb{Q}$ rather free of content. Instead, it is very well possible that $f = f_0\psi$ is obtained from a defining equation $f_0 \in \mathbb{Q}[x, y]$ for X by means of some complicated coordinate transformation ψ with coefficients in $\mathbb{C}$. In this case there is no longer any reason to suspect that f belongs to $\mathbb{Q}[x, y]$, even though it (and therefore corresponding algebraic curve) can certainly be transformed to a form over $\mathbb{Q}$ by means of the (usually unknown) transformation φ^{-1}.

How do we find such an equation $f_0 \in \mathbb{Q}[x, y]$ when we are only given $f \in \mathbb{C}[x, y]$? Indeed, when is it reasonable to suspect that such an $f_0 \in \mathbb{Q}[x, y]$ exists at all? To answer the second question, we note that if X is indeed defined by

same equation $f_0\psi$ with $f_0 \in \mathbb{Q}[x,y]$, then $\sigma(X)$ is defined by

$$\sigma(f) = \sigma(f_0\psi) = \sigma(f_0)\sigma(\psi) = f_0\sigma(\psi), \tag{34}$$

so that applying the (in general non-trivial) transformation $\varphi_\sigma = \psi^{-1}\sigma(\psi)$ maps X isomorphically to $\sigma(X)$. We therefore see that our question is not one of equality, but of ISOMORPHISM.

Motivated by the Galois theory above, it now stands to reason to suspect that X_0 admits a defining equation over $\mathbb{Q}$ if and only if there exists isomorphisms

$$\varphi_\sigma : X \to \sigma(X) \tag{35}$$

for all $\sigma \in \mathrm{Aut}(\mathbb{C}|\mathbb{Q})$. Yet surprisingly enough, this is **not** true. Counterexamples were first constructed independently of each other by Earle and Shimura. A particularly simple one is provided by

$$X : y^2 = x^6 + ix^4 + x^3 - ix^2 + 1. \tag{36}$$

This curve is isomorphic to its complex conjugate under the rational map

$$(x,y) \mapsto (1/x, y/x^3). \tag{37}$$

Yet despite this invariance under complex conjugation up to isomorphism, there does **not** exist a defining equation of X with coefficients in $\mathbb{R}$.

The study of this peculiar phenomenon is known as GALOIS DESCENT; at its most abstract, it involves the study of abstruse cohomological objects called GERBES.[4] Spelling out this theory, as well as providing concrete criteria for descent, is a versatile topic for a PhD thesis.

6 Exercise for Chapter VI

Exercise 1. Show that Galois' criterion at the end of Section 3 does not apply if the degree of f is not prime.

Exercise 2. (This exercise was suggested by Jaap Top.) Let $L|K$ be a separable field extension, and let $N|K$ be its normal closure from Exercise I.12. Show that there exists an ascending chain

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n = L$$

whose successive extension degrees $[K_{i+1} : K_i]$ are at most d if and only if the Galois group $G = \mathrm{Gal}(N|K)$ admits a descending chain

$$G =:= H_0 \supset H_1 \supset \ldots \supset H_{n-1} \supset H_n = \{e\}$$

whose successive indices $[H_i : H_{i+1}]$ are at most d.

[4] See https://en.wikipedia.org/wiki/Gerbe [Accessed 16 May 2024]

Chapter VII

Projects for further study

This chapter describes a number of projects for further exploration in the realm of Galois theory. Besides expanding your theoretical knowledge, they also consider the implementation of the corresponding results in computer algebra systems.

1 Stauduhar's algorithm

This first project deals with the generalization of the methods from Sections V.1 and V.2 to compute the Galois groups of quintic separable irreducible polynomials of degree 5. As in these sections, we start by classifying the possible Galois groups.

Proposition 1.1. *Let $G \subset S_5$ be a transitive subgroup. Then exactly one of the following statements holds true.*

(i) *G is conjugate to $\langle (1\ 2\ 3\ 4\ 5) \rangle \simeq C_5$.*

(ii) *G is conjugate to $\langle (1\ 2\ 3\ 4\ 5), (1\ 4)(2\ 3) \rangle \simeq D_5$.*

(iii) *G is conjugate to $\{(1\ 2\ 3\ 4\ 5), (1\ 2\ 4\ 3)\} =: F_{20}$.*

(iv) *$G = A_5$.*

(v) *$G = S_5$.*

*Proof**. As in the proof of Proposition 1.1, we see that G must contain a 5-cycle σ after renumbering. We moreover define $H \subset G$ to be the stabilizer of 5 under the action of G on $\{1,2,3,4,5\}$; since said action is transitive, the orbit-stabilizer theorem shows that H is of index 5 in G. We can interpret H as a subgroup of S_4 via its action on $\{1,2,3,4\}$, and we have $G = \langle \sigma, H \rangle$. Indeed, we certainly have $\langle \sigma, H \rangle \subset G$ and since $\langle \sigma \rangle$ acts transitively on $\{1,2,3,4,5\}$, we can, given an element $g \in G$, find a power σ^i such that $h = \sigma^i g$ fixes 5. Therefore $h \in H$ and $g = \sigma^{-i} h$ belongs to $\langle \sigma, H \rangle$, which shows that the converse inclusion holds as well.

Suppose first that H contains a 2-cycle τ. After renumbering, we may assume that $\sigma = (1\ 2\ 3\ 4\ 5)$ and that $\tau = (1\ i)$ for some i with $2 \leq i \leq 4$. Since p is a prime number, all non-trivial powers of σ generate the same group as σ, so that we may as well replace σ by its $(i-1)$-th power, which is of the form $(1\ i\ \cdots)$. Another renumbering then allows us to assume that $\sigma = (1\ 2\ \cdots\ p)$ and $\tau = (1\ 2)$. In this case G also contains the conjugates $(2\ 3), \ldots, (p-1\ p)$ of $(1\ 2)$ under powers of σ, and the proof that S_n is generated by its 2-cycles for any $n \geq 1$ equally well shows that these 2-cycles generate all of S_5.

Now suppose that H contains a 3-cycle τ. After renumbering, we may assume that $\tau = (1\ 2\ 3)$. Since the 5-cycle σ already acts transitively on $\{1,2,3,4,5\}$, one of its powers π maps 4 to 5. It therefore cannot map 5 to 5 as well, but neither can it map 5 to 4, because being a non-trivial power of a 5-cycle, π is again a 5-cycle. If we conjugate τ by this π, then τ is sent to another 3-cycle τ' such that the support of τ' is the complement of $\{\sigma(4), \sigma(5)\} = \{5, \sigma(5)\}$. Since $\sigma(5) \notin \{4,5\}$, the support of τ is contained in $\{1,2,3,4\}$, but does not coincide with that of τ. Therefore H contains $\langle \tau, \tau' \rangle$, and this is a transitive subgroup of A_4. Since H contains the 3-cycle τ, Proposition 2.1 implies that H contains A_4, so that it equals either A_4 or S_4.

If $H = S_4$, then we have $G = S_5$, for example because H again contains a 2-cycle. If $H = A_4$, then since the permutations in A_4 are even, and the same is the case for σ, we see that $G = \langle H, \sigma \rangle$ is contained in A_5. Since $\#G = 5 \cdot \#H = 5 \cdot 12 = 60 = (5!)/2 = \#A_4$, we see that then in fact $G = A_5$. Since these are normal subgroups of S_5, they are not affected by our choices of numbering.

Now let us suppose first that H is non-transitive. Then its action partitions $\{1,2,3,4\}$ into proper subsets. If one of these subsets is of cardinality 1, then after a suitable renumbering we obtain that H contained in S_3. Since we have already considered the case where H contains a 2-cycle or a 3-cycle, the only remaining possibility is that H is trivial, in which case is generated by the 5-cycle σ that it contains as $\langle \sigma \rangle \subset G$ and $\#\langle \sigma \rangle = 5 = 5\#H = \#G$.

The remaining possibility in the intransitive case is that the action of H partitions $\{1,2,3,4\}$ into two subsets of order 2. There are two ways in which this can happen; also see Exercise V.1. The first is for H to contain two disjoint 2-cycles, a case that we have once again already dealt with. The second is for H to be generated by a $(2,2)$-cycle τ.

In the latter case, G is a group of order $2 \cdot 5$, and it is non-abelian since S_5 does not contain an element of order 10. Since 5 is prime, we see that G is isomorphic to D_5. Renumbering as above, we obtain that the cyclic group generated by $\sigma = (1\ 2\ 3\ 4\ 5)$ is a normal subgroup of H. It is therefore sent to itself under conjugation with τ. Now τ cannot commute with σ, since otherwise G would be abelian. Since conjugation by τ twice amounts to conjugation by $\tau^2 = e$, we obtain the fourth equality in the chain

$$\begin{aligned}(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ 5) = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5)) = \tau(1\ 2\ 3\ 4\ 5)\tau^{-1} \\ = \tau\sigma\tau^{-1} = \sigma^{-1} = (1\ 5\ 4\ 3\ 2) = (4\ 3\ 2\ 1\ 5),\end{aligned} \tag{1}$$

so that $\tau = (1\ 4)(2\ 3)$. While we do not in fact need this further information on τ to conclude that $G \simeq D_5$, it will help us to deal with the remaining possibilities for H.

Indeed, we have now reduced to the case where H is transitive, so that we can use Proposition 2.1. Having already dealt with the cases $H = A_4$ and $H = S_4$, we check which remaining possibilities can occur. First suppose that H contains the subgroup V_4, so that either $H = V_4$ or $H = D_4$. After renumbering $\{1, 2, 3, 4\}$, which does not affect the elements of V_4, we may assume that $\sigma = (1\ 2\ 3\ 4\ 5)$. We then see that H contains the 3-cycle

$$\sigma(1\ 2)(3\ 4)\sigma(1\ 3)(2\ 4)\sigma = (1\ 5\ 2), \tag{2}$$

so that we are again reduced to one of the cases above; we have $G = A_5$.

The capstone of the proof is therefore the case where $H \simeq C_4$ is generated by a 4-cycle τ. In this case τ^2 is a $(2,2)$-cycle. Assuming that $\sigma = (1\ 2\ 3\ 4\ 5)$ as before, the discussion around (1) shows that $\tau^2 = (1\ 4)(2\ 3)$, which implies that τ equals either $(1\ 2\ 4\ 3)$ or its inverse $(1\ 3\ 4\ 2)$. As these 4-cycles generate the same group $H \subset S_4$, we may as well take τ to be the former.

Now if there exists a group $G \subset S_5$ containing σ such that $H = \langle \tau \rangle$ at all, then we must have $G = \langle \sigma, H \rangle = \langle \sigma, \tau \rangle$. To show conversely that $G := \langle \sigma, \tau \rangle$ is indeed a subgroup of S_5 with $G \cap S_4 = H$, it suffices to prove that

$$G = \left\{ \sigma^i \tau^j : 0 \le i \le 4, 0 \le j \le 3 \right\}. \tag{3}$$

Indeed, if (3) holds, then given an element $g = \sigma^i \tau_j$ on the right hand side of (3) we have $g(5) = \sigma^i \tau^j(5) = \sigma^i(5)$, so that an element $\sigma^i \tau^j$ belongs to $G \cap S_4$ if and only if $\sigma^i(5) = 5$. This happens if and only if $5 \mid i$, in which case $g = \tau^j \in H$.

Since $G = \langle \sigma, \tau \rangle$, the elements of the right hand side of (3), which we shall briefly baptize R, are in G. To show the converse, it is enough to prove that R is indeed a group, and to this end we first observe that

$$\tau\sigma\tau^{-1} = \tau(1\ 2\ 3\ 4\ 5)\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5)) = (2\ 4\ 1\ 3\ 5) = \sigma^2 \tag{4}$$

and similarly

$$\tau^{-1}\sigma\tau = (\tau^{-1}(1)\ \tau^{-1}(2)\ \tau^{-1}(3)\ \tau^{-1}(4)\ \tau^{-1}(5)) = (3\ 1\ 4\ 2\ 5) = \sigma^3. \tag{5}$$

We now check the group axioms for R. Taking $i = j = 0$ in (3), we see that $e \in R$, and given two elements $\sigma^{i_1}\tau^{j_1}$ and $\sigma^{i_2}\tau^{j_2}$ of R, repeated application of (4) shows the third equality in the chain

$$\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2} = \sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{-j_1}\tau^{j_1}\tau^{j_2} = \sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{-j_1}\tau^{j_1}\tau^{j_2} = \sigma^{i_1+2^{j_1}i_2}\tau^{j_1+j_2}, \tag{6}$$

which is again an element of R; after all, since $\mathrm{ord}(\sigma) = 5$ and $\mathrm{ord}(\tau) = 4$, we have

$$\begin{aligned} \sigma^{i_1+2^{j_1}i_2} &\in \langle \sigma \rangle = \left\{ \sigma^i : 0 \le i \le 4 \right\} \quad \text{and} \\ \tau^{j_1+j_2} &\in \langle \tau \rangle = \left\{ \tau^j : 0 \le j \le 3 \right\}. \end{aligned} \tag{7}$$

Similarly, (5) shows that given an element $\sigma^i\tau^j$ of R we have

$$(\sigma^i\tau^j)^{-1} = \tau^{-j}\sigma^{-i} = \sigma^{-3^j i}\tau^{-j}, \tag{8}$$

which is again in R. Therefore the group G is indeed a subgroup of S_5 with $G \cap S_4 = \langle \tau \rangle$, and it yields the final entry F_{20} in the statement of the proposition.

Note that the orbit-stabilizer theorem implies that $\#G = 5\#H = 5 \cdot 4 = 20$. As in all other cases above, the fact that we renumbered the elements of $\{1,2,3,4,5\}$ implies that other subgroups G of S_5 such that $\#G = 20$ need not equal F_{20}, but the proof shows that any such group is conjugate to F_{20}, and therefore in particular isomorphic to it. ♡

Remark 1.2. Using the Sylow theorems, the proof of Proposition 1.1 becomes easier, as said theorem implies that if H is neither of the groups A_5 and S_5, then $N = \langle \sigma \rangle$ is a normal subgroup of G; the fact that N is normalized by H then implies, as in (1), that if $\sigma = (1\ 2\ 3\ 4\ 5)$, then $(1\ 4)(2\ 3)$ is the only $(2,2)$-cycle in S_5 that can be contained in H. This obviates the need for the somewhat incomprehensible trick in (2).

In fact this reasoning gives the group F_{20} (which is also called the FROBENIUS GROUP of order 20) the structure of a so-called SEMIDIRECT PRODUCT, which yields a more intrinsic explanation of the miraculous conjugation relation (4), which can be understood as the square root of the action $\sigma \mapsto \sigma^{-1}$ by the group $C_2 \simeq D_5/D_5^+$ that is induced by the conjugation action of D_5 on itself. ❁

Now let a separable irreducible quintic polynomial $f \in K[x]$ be given. Our goal is to be able to determine the group $G = \mathrm{Gal}(f)$ by using the classification in Proposition 1.1. By Theorem V.1.7, the discriminant $\Delta(f)$ already allows us to decide whether $G \subset A_5$. We want to do the same for the conjugates of the next largest group F_{20} in Proposition 1.1. To make this possible, we formulate a common generalization of the constructions from Definitions V.1.2 and V.2.6.

Definition 1.3. Let $R = K[x_1, \dots, x_n]$, and let H be a subgroup of S_n. We say that a polynomial $f \in R$ is an EXACT H-INVARIANT if we have

$$S(f) = H \tag{9}$$

for the stabilizer of f under the action of S_n on R from Proposition V.3.1. ✌

Exact H-invariants exist for any subgroup $H \subset S_n$, and as the following theorem shows, they can even be constructed explicitly.

Theorem 1.4. *Let H be a subgroup of S_n. Then there exists a monomial $\mathbf{x}^{\mathbf{i}}$ such that the sum*

$$I(\mathbf{x}^{\mathbf{i}}) = \sum_{\sigma \in H} \sigma(\mathbf{x}^{\mathbf{i}}) \tag{10}$$

is an exact H-invariant; in particular, one can take $\mathbf{x}^{\mathbf{i}} = x_1 x_2^2 \cdots x_n^n$.

We can now further symmetrize to obtain a polynomial over the ground field, as in Definition V.2.6 and Proposition V.2.11.

Theorem 1.5 (Stauduhar)**.** *Let $f \in K[x]$ be a separable polynomial of degree n, and let $G = \mathrm{Gal}(f)$, considered as a subgroup of S_n by labeling the zeros of*

$$f = \alpha(x - \beta_1) \cdots (x - \beta_n). \tag{11}$$

Finally, let $H \subset S_n$ be a subgroup, and let I be an exact H-invariant.

(i) *The* RESOLVENT POLYNOMIAL

$$\rho_I(f) = \prod_{\sigma H \in S_n/H} (x - \sigma(I(\beta_1, \ldots, \beta_n))) \in L[x] \tag{12}$$

associated to I is in fact an element of $K[x]$.

(ii) *If $\rho_I(f)$ is separable, then G is contained in an S_n conjugate of H if and only if $\rho_I(f)$ has a zero in K.*

(iii) *If additionally $K = \mathbb{Q}$ and $f \in \mathbb{Z}[x]$ is monic, then the equivalent conditions in (ii) hold if and only if $\rho_I(f)$ has a zero in $\mathbb{Z}$.*

Remark 1.6. The polynomial $\rho_I(f)$ in (12) is well-defined; because I is an H-invariant of $K[x]$, an equality of cosets $\sigma H = \sigma' H$ yields

$$\sigma(I(\beta_1, \ldots, \beta_n)) = I(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) = (\sigma I)(\beta_1, \ldots, \beta_n) = I(\beta_1, \ldots, \beta_n). \tag{13}$$

❁

Using the methods of Example 3.4(ii), one can given I obtain an explicit expression for the associated resolvent polynomial $\rho_I(f)$ in terms of the coefficients of f itself. In our current situation, we are interesting in the case $H = F_{20}$. In this case, we have the following result.

Proposition 1.7. *Let $\mathbf{x}^{\mathbf{i}} = x_1^2 x_2 x_3$. Then $I(\mathbf{x}^{\mathbf{i}})$ is an exact F_{20}-invariant. Moreover, the polynomial $\rho_I(f)$ is generically separable, in the sense that it is separable for the polynomial $f = (x - x_1) \cdots (x - x_n)$ with coefficients in the rational function field $K(x_1, \ldots, x_n)$.*

We call the resolvent polynomial from Proposition 1.7 the RESOLVENT SEXTIC of f. Combining this proposition with Theorem 1.5 and Proposition 1.1, we obtain the following result.

Theorem 1.8. *Let K be a field with $\mathrm{char}(K) \neq 2$, let $f \in K[x]$ be a separable irreducible quintic polynomial with discriminant Δ and resolvent sextic ρ. Suppose that ρ is separable as well. Then the following statements hold.*

(i) *If Δ is not a square in K and ρ has no zero in K, then $\mathrm{Gal}(f) \simeq S_5$.*

(ii) *If Δ is a square in K and ρ has no zero in K, then $\mathrm{Gal}(f) \simeq A_5$.*

(iii) *If Δ is not a square in K and ρ has a single zero in K, then $\mathrm{Gal}(f) \simeq F_{20}$.*

(iv) *If Δ is a square in K, and ρ has a single zero in K, and f does not split into linear factors over its stem field, then $\mathrm{Gal}(f) \simeq D_5$.*

(v) *If Δ is a square in K, and ρ has a single zero in K, and f splits into linear factors over its stem field, then $\mathrm{Gal}(f) \simeq C_5$.*

Theorem 1.8 is somewhat unsatisfying, in the sense that distinguishing between D_5 and C_5 still requires us to factor polynomials over the quintic field stem field of f. After all, a recurring theme of these notes has been the reduction of calculations to the base field. The same problem occurred for

quartic polynomials; see Remark V.2.10. In the remainder of this section, we indicate how we can get around it in the quintic case when $K = \mathbb{Q}$.

Suppose therefore that $f \in \mathbb{Q}[x]$ is a separable irreducible quintic polynomial whose Galois group equals either D_5 or C_5. Over the field of complex numbers $\mathbb{C}$, we can use Newton approximation to effectively determine a factorization

$$f = \alpha(x-\beta_1)\cdots(x-\beta_n) \tag{14}$$

to arbitrary precision, and with it an embedding of $G = \mathrm{Gal}(f)$ into S_5. Theorem 1.8 shows that the sextic resolvent ρ of f has a zero by our assumption on the Galois group of f, and Theorem 1.5(iii) shows that this zero is in fact an element of $\mathbb{Z}$. Since the zeros of $\rho_I(f)$ are obtained from each other by relabeling the indices of the β_i, we may perform exactly such a relabeling to assume that the zero of $\rho_I(f)$ in $\mathbb{Z}$ is the element

$$\begin{aligned}\beta_1^2\beta_2\beta_3 + \beta_1^2\beta_2\beta_4 + \beta_1^2\beta_3\beta_5 + \beta_1^2\beta_4\beta_5 + \beta_1\beta_2^2\beta_4 + \beta_1\beta_2^2\beta_5 + \beta_1\beta_2\beta_3^2 \\ + \beta_1\beta_2\beta_5^2 + \beta_1\beta_3^2\beta_4 + \beta_1\beta_3\beta_4^2 + \beta_1\beta_3\beta_5^2 + \beta_1\beta_4^2\beta_5 + \beta_2^2\beta_3\beta_4 \\ + \beta_2^2\beta_3\beta_5 + \beta_2\beta_3^2\beta_5 + \beta_2\beta_3\beta_4^2 + \beta_2\beta_4^2\beta_5 + \beta_2\beta_4\beta_5^2 + \beta_3^2\beta_4\beta_5 + \beta_3\beta_4\beta_5^2\end{aligned} \tag{15}$$

that is fixed by the exact subgroup $H = F_{20}$, thus ensuring that $G \subset H$, which this time is an actual inclusion (not merely an inclusion up to conjugation). We now have the following result.

Proposition 1.9. *The subgroup $H = F_{20}$ of S_5 has a unique subgroup of order 5, namely $H' = \langle(1\ 2\ 3\ 4\ 5)\rangle$.*

To determine whether $\mathrm{Gal}(f)$ is cyclic or dihedral it, it suffices in light of Proposition 1.9 to determine whether it is contained in H' or not. We do this by means of another resolvent polynomial, though this time we refine the process by symmetrizing the resolvent polynomial over H instead of over S_5. We accordingly define

$$I'(\mathbf{x}^\mathbf{i}) = \sum_{\sigma\in H} \sigma(\mathbf{x}^\mathbf{i}) \tag{16}$$

for $\mathbf{x}^\mathbf{i} = x_1^2x_2$, as well as the associated resolvent

$$\rho_{I'}(f) = \prod_{\sigma H'\in H/H'} (x - \sigma(I(\beta_1,\dots,\beta_n))) \in \mathbb{C}[x]. \tag{17}$$

We now have the following analogue of Proposition 1.7.

Proposition 1.10. *The polynomial $\rho_{I'}(f)$ is generically separable, in the sense that it is separable for the polynomial $f = (x-x_1)\cdots(x-x_n)$ with coefficients in the rational function field $K(x_1,\dots,x_n)$.*

We can now decide whether $\mathrm{Gal}(f)$ is contained in H' or not, and thus decide whether $\mathrm{Gal}(f) \simeq C_5$ or $\mathrm{Gal}(f) \simeq D_5$, in terms of the resolvent $\rho_{I'}(f)$.

Theorem 1.11. *Let $f \in K[x]$ be a separable polynomial of degree 5, and let $G = \mathrm{Gal}(f)$, considered as a subgroup of S_n by labeling the zeros of*

$$f = \alpha(x-\beta_1)\cdots(x-\beta_5). \tag{18}$$

Suppose that $G \subset F_{20}$. Then the following statements hold.

(i) *We have* $\rho_{I'}(f) \in \mathbb{Q}[x]$, *and if* $f \in \mathbb{Z}[x]$ *is monic, then it belongs to* $\mathbb{Z}[x]$.

(ii) *If* $\rho_{I'}(f)$ *is separable, then* G *is contained in* H' *if and only if* $\rho_{I'}(f)$ *has a zero in* K.

(iii) *If* $f \in \mathbb{Z}[x]$ *is monic, then the equivalent conditions in (ii) hold if and only if* $\rho_{I'}(f)$ *has a zero in* $\mathbb{Z}$, *in which case* $\rho_{I'}(f)$ *even splits into linear factors over* $\mathbb{Z}$.

This theorem concludes your upcoming odyssey, or at least it shows the islands that it will visit. You may now use the following exercises, or a proper subset of your choice, as a guide to your exploration of this theme.

Exercise 1. Prove Theorem 1.4.

Exercise 2. Prove Theorem 1.5.

Exercise 3. Prove Proposition 1.7.

Exercise 4. Prove Theorem 1.8.

Exercise 5. Prove Proposition 1.9.

Exercise 6. Prove Proposition 1.10.

Exercise 7. Prove Theorem 1.11.

Exercise 8. Let $f = a(x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x^1 + a_5) \in K[x]$ be a quintic polynomial, and let $\rho_I(f)$ be its resolvent sextic. Determine the coefficients of $\rho_I(f)$ as zeros of $\rho_I(f)$ as polynomial expressions in the a_i.

Exercise 9. Let $f \in \mathbb{Q}[x]$ be a separable quintic polynomial with discriminant Δ and sextic resolvent ρ. Show that if Δ is a square in K, and ρ has a single zero in K, and f does not split into linear factors over $\mathbb{R}$, then $\mathrm{Gal}(f) \simeq D_5$.

Exercise 10. For each of the following pairs K and f, determine the Galois group of the polynomial $f \in K[x]$. You may use that f is separable and irreducible in all cases.

(i) $K = \mathbb{Q}$, $f = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$.

(ii) $K = \mathbb{Q}$, $f = x^5 - 2x^4 + 2x^3 - x^2 + 1$.

(iii) $K = \mathbb{Q}$, $f = x^5 - x^4 + 2x^3 - 4x^2 + x - 1$.

(iv) $K = \mathbb{Q}$, $f = x^5 - x^4 + 2x^2 - 2x + 2$.

(v) $K = \mathbb{Q}$, $f = x^5 - x^3 - x^2 + x + 1$.

Exercise 11. Discuss how the results in [Dum91] relate to the techniques in the current section.

Exercise 12. Write algorithms in SageMath that implement the results in this section to determine the Galois group of a separable irreducible quintic $f \in K[x]$, either over $K = \mathbb{Q}$ or over general fields, as you prefer.

Vista

If you have been paying close attention, then you may have realized that our argumentation after Theorem 1.8 involves a rather questionable practice: We have used approximations of the roots β_i in $\mathbb{C}$, which always has to be done with some care. And indeed, in Theorem 1.11 it is not immediately clear how to compute $\rho_{I'}(f)$ over $\mathbb{Q}$, as we cannot use the theory of symmetric polynomials from Section III.3, having symmetrized over F_{20} instead of over the larger group S_5. We can of course always compute $\rho_{I'}(f)$ and determine its possible integral zeros purely over $\mathbb{C}$, but this requires justification, since whatever our precision, we cannot say whether an element of $\mathbb{C}$ belongs to $\mathbb{Z}$ or is instead a complicated algebraic number from its approximation only.

The current way to solve the problem sketched in the previous paragraph is an elegant combination of the aforementioned computation over $\mathbb{Q}$ with a complementary computation over the p-ADIC NUMBERS. This is beyond the scope of these notes, but a good description of the state of the art can be found in [FK14]. This method involves the systematic iterative determination of further and further resolvents until the Galois group of a given polynomial f of arbitrary degree is known, by means of calculations that take place over its base field. This constellation of results is sometimes called STAUDUHAR'S ALGORITHM, after Richard Stauduhar, who led the way in his 1969 PhD thesis, the results of which were published in [Sta73].

2 Cebotaryov's theorem

The previous section shows that determining a Galois group can be quite complicated. Current methods typically need to evaluate quite a few resolvents to determine complicated Galois groups. This is somewhat disheartening. However, the good news is that the Galois group of a separable irreducible polynomial $f \in K[x]$ of degree n can often still be calculated quickly provided that it be large, say S_n or A_n.

In this section, we consider the methods that makes this possible for the base field $K = \mathbb{Q}$. For this, we need the following result by Dedekind, which we do not prove, as this involves the theory of number rings.

Theorem 2.1 (Dedekind). *Let $f \in \mathbb{Z}[x]$ be a separable polynomial of degree n, and let $G = \mathrm{Gal}(f)$, considered as a subgroup of S_n. Let p be a prime that does not divide the leading coefficient of f, and suppose that the reduction $\overline{f} \in \mathbb{F}_p[x]$ of f modulo p is separable. If we factor*

$$\overline{f} = g_1 \cdots g_r \in \mathbb{F}_p[x] \tag{19}$$

into irreducible polynomials g_i in $\mathbb{F}_p[x]$, then G contains an element σ whose cycle type equals $(\deg(g_1), \ldots, \deg(g_r))$.

Now there exist efficient algorithms to factor the reduced polynomial $\overline{f} \in \mathbb{F}_p[x]$; this is not by any means obvious, but we refer to a course on algorithmic algebra for more information, and you may use such algorithms as a black box in your own project. Thus, Theorem 2.1 will often show the existence of elements

in G with a certain cycle type, and often this in itself is enough to determine G, as the upcoming propositions show.

Proposition 2.2. *Let p be a prime, and let $G \subset S_p$ be a subgroup. If G contains both a p-cycle and a 2-cycle, then $G = S_p$.*

Proof. Let σ (respectively τ) be the p-cycle (respectively the 2-cycle) under consideration. After renumbering, we may assume that $\sigma = (1\ \cdots\ p)$ and $\tau = (1\ i)$ for some $i \geq 2$. Since p is a prime number, all non-trivial powers of σ generate the same group as σ, so that we may as well replace σ by its $(i-1)$-th power, which is of the form $(1\ i\ \cdots)$. Another renumbering then allows us to assume that $\sigma = (1\ 2\ \cdots\ p)$ and $\tau = (1\ 2)$. In this case G also contains the conjugates $(2\ 3), \ldots, (p-1\ p)$ of $(1\ 2)$ under powers of σ, and the proof that S_n is generated by its 2-cycles for any $n \geq 1$ equally well shows that these 2-cycles generate all of S_p. ♡

Remark 2.3. The hypothesis is in Proposition 2.2 that p be prime is necessary: The transitive subgroup D_4 in Proposition V.2.1 contains both 4-cycles and 2-cycles, but does not equal S_4. ❁

Proposition 2.4. *Let $G \subset S_n$ be a transitive subgroup. If G contains both an $(n-1)$-cycle and a 2-cycle, then $G = S_n$.*

Proof. Let σ (respectively τ) be the $n-1$-cycle (respectively the 2-cycle) under consideration. After renumbering, we may assume that $\sigma = (1\ \cdots\ n-1)$ and $\tau = (i\ j)$ say. Since G is transitive, there exists some element of G that maps i to n. Conjugating τ accordingly, we obtain a new 2-cycle $\tau' = (i'\ n)$ in G. Subsequently conjugating τ' by the powers of σ, we obtain the 2-cycles $(1\ n), \ldots, (n-1\ n)$, which generate S_n, as was mentioned in the proof of Proposition 2.2. ♡

Remark 2.5. The hypothesis is in Proposition 2.2 that G be transitive is necessary: Considering S_3 as a subgroup of S_4, we have that S_3 contains the 3-cycle $(1\ 2\ 3)$ as well as the 2-cycle $(1\ 2)$, but $S_3 \neq S_4$. ❁

A natural question is: If $f \in \mathbb{Q}[x]$ is a separable irreducible polynomial with Galois group S_n, how many primes will we have to sample before we can apply Proposition 2.2 or Proposition 2.4? In other words: Can we reasonable predict what proportion of primes given rise to n-cycles or $(n-1)$-cycles in Theorem 2.1? The answer to this question comes from the following theorem.

Theorem 2.6 (Chebotaryov). *Let $f \in \mathbb{Z}[x]$ be a separable polynomial of degree n, and let $G = \mathrm{Gal}(f)$, considered as a subgroup of S_n. Given a cycle type t, the* DENSITY *d_t of the set $T \subset \mathbb{P}$ of primes p such that the cycle type of the reduction modulo p equals t is given by*

$$d_t = \frac{\#\{g \in G : g \text{ has cycle type } t\}}{\#G}. \tag{20}$$

In particular, one has

$$\lim_{N\to\infty} \frac{\#(T \cap \{1,\ldots,N\})}{\#(\mathbb{P} \cap \{1,\ldots N\})} = \frac{\#\{g \in G : g \text{ has cycle type } t\}}{\#G}. \tag{21}$$

Moreover, if a cycle type does not occur in G, then no reduction of f modulo a prime will give rise to it p.

Theorem 2.6 often allows one to determine the Galois group of a polynomial in $\mathbb{Z}[x]$ by analyzing the frequencies of the various cycle types that it gives rise to, as is shown by the following example.

Example 2.7. (i) Theorem 2.6 implies that the density of the set of primes modulo which f splits into linear factors equals $1/\#G$. Thus the cardinality of the Galois group of f can be determined by means of Theorem 2.1, at least heuristically.

(ii) If $\mathrm{Gal}(f) \in S_n$ in Theorem 2.6, then the frequencies of an n-cycle (respectively of an $n-1$-cycle and of a 2-cycle) equals n^{-1} (respectively $(n-1)^{-1}$ and $(2(n-1)!)^{-1}$).

(iii) If $\deg(f) = 4$ and $\mathrm{Gal}(f) \simeq C_4$, then Theorem 2.6 implies that reducing f modulo p will given rise to a 4-cycle half of the time, whereas $(2,2)$-cycles occur with probability 1/4. Finally, the probability that f splits into linear factors modulo p equals 1/4.

(iv) If $\deg(f) = 4$ and $\mathrm{Gal}(f) \simeq V_4$, then Theorem 2.6 implies that reducing f modulo p will given rise to a $(2,2)$-cycle with probability 3/4. Moreover, the probability that f splits into linear factors modulo p equals 1/4. ❀

We from Example 2.7(iii)-(iv) that the reductions of f can tell the Galois groups C_4 and V_4 of cardinality 4 apart, at least heuristically; if $\mathrm{Gal}(f) \simeq C_4$, then eventually we will find some prime p modulo which it is irreducible, whereas this will never happen if $\mathrm{Gal}(f) \simeq V_4$.

You may now use the following exercises, or a proper subset of your choice, as a guide to your exploration of this theme.

Exercise 13. Let p be a prime, and let $f \in \mathbb{Q}[x]$ be a separable irreducible polynomial of degree p that has exactly $p-2$ roots in $\mathbb{R}$. Show that $\mathrm{Gal}(f) = S_p$.

Exercise 14. Write algorithms in `SageMath` that given a polynomial $f \in \mathbb{Q}[x]$ samples prime numbers p and uses the associated reductions of f to show that $\mathrm{Gal}(f) = S_n$ with the help of Theorem 2.1 as well as Propositions 2.2 and 2.4.

Exercise 15. Prove the statements in Example 2.7.

Exercise 16. Write algorithms in `SageMath` that distinguish polynomials of polynomials degree 4 by means of a frequency analysis of the various cycle types that one obtains on reduction.

Exercise 17. The same question as the previous one, but this time with polynomials of degree 5; see Proposition 1.1.

Exercise 18. Add Bayesian estimators to the algorithms in the previous questions, so that they terminate as soon as the likelihood a posteriori of the Galois group that is returns is below any specified small positive bound.

Vista

Theorem 2.6 admits a more precise version, in terms of the FROBENIUS ELEMENTS of G at the various primes p. Such elements are lifts to $\mathrm{Gal}(f) = \mathrm{Gal}(L|\mathbb{Q})$ of the Frobenius automorphisms on the quotient of the ring of integers $\mathbb{Z}_L$ by its various primes $\mathfrak{p}$ over p. Given p, there turns out to be a unique such lift σ_p as long as f is separable modulo p, but there is a remaining ambiguity, as there is still a choice of the prime $\mathfrak{p}$ involved in its construction. One can show that changing $\mathfrak{p}$ affects σ_p up to a conjugation in G only. Therefore we can meaningfully determine the G-conjugacy class of σ_p, and not merely its cycle type, which amounts to its S_n-conjugacy class.

Chebotaryov's result then states that the various σ_p are equidistributed among the conjugacy classes in G, in the sense that the density of the set of primes p for which σ_p belongs to a given conjugacy class X in G (which is well-defined in light of the previous paragraph, even if σ_p is not) equals $\#X/\#G$. This version of Theorem 2.6 can be proved by using class field theory, and has important consequences in this theory as well; also see Section VI.3.

3 Solvability by radicals (for real)

The final theme of this chapter is an elaboration on the problems and techniques around solvable extensions that led to the development of Galois theory, as discussed in Section VI.2. In that section, we gave a criterion under which a polynomial equation $f(x) = 0$ over $\mathbb{Q}$ admits a solution by means of radicals in terms of the Galois group G of f; we needed G to satisfy the following property.

Definition 3.1. Let G be a finite group. Then G is called SOLVABLE if there exists a descending chain of subgroups

$$G =: H_{-1} \supset H_0 \supset H_1 \supset \ldots \supset H_{n-1} \supset H_n = \{e\} \tag{22}$$

with the property that H_i is normal in H_{i-1} with abelian quotient H_{i-1}/H_i for $i = 0, \ldots n$. ✌

Two logical questions remain:

(i) Can we decide effectively whether a given finite group G is solvable?

(ii) If $G = \mathrm{Gal}(f)$ is solvable, can we determine which radicals are needed to construct the corresponding field extension?

We start with Question (i), which can be decided with a very explicit notion.

Definition 3.2. Let G be a finite group. The COMMUTATOR SUBGROUP $G^{(1)} = [G, G]$ of G is the subgroup of G that is generated by all elements of the form

$$[g, h] = ghg^{-1}h^{-1} \tag{23}$$

We define the DERIVED SERIES of G to be the descending chain

$$G =: G^{(0)} \supset G^{(1)} \supset \ldots \supset G^{(i-1)} \supset G^{(i)} \supset \ldots \tag{24}$$

where $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ for $i > 0$. ✌

It turns out that whether a finite group G is abelian or not can be decided purely in terms of the derived series of G.

Theorem 3.3. *Let G be a finite group. Then the following statements hold.*

(i) *$[G,G]$ is a normal subgroup of G and the quotient group $G/[G,G]$ is abelian.*

(ii) *If N is another normal subgroup of N such that G/N is abelian, then N contains $[G,G]$.*

(iii) *G is solvable if and only if the derived series of G terminates in the trivial subgroup $\{e\}$.*

We now pass to Question (ii) above. If G is solvable, then any series of the form (22) can be refined to a series in which the successive quotients H_{i-1}/H_i are cyclic. We aim to describe the corresponding subextension

$$L_i \,|\, L_{i-1} \tag{25}$$

by means of radicals.

Note that by construction $L_i \,|\, L_{i-1}$ is a Galois extension, and that its Galois group $\mathrm{Gal}(L_i \,|\, L_{i-1})$ is cyclic. Given i, we can determine L_i explicitly, for example as a subfield of the splitting field L of f (which you may assume to be available; we are cheating here to some extent, but be that as it may); see Exercise 21. We may therefore as well assume that $L_i = L$ and $L_{i-1} = K$.

Now let $n = [L : K]$, and let us moreover assume that K contains a primitive n-th root of unity ζ_n, as we may by Theorem 4.5. Our goal is to prove the following statement.

Theorem 3.4. *Let $L \,|\, K$ be a finite Galois extension of fields of characteristic zero. Suppose that $\mathrm{Gal}(L \,|\, K)$ is cyclic of order n, generated by an automorphism σ. If K contains a primitive n-th root of unity ζ_n, then there exists an element $\beta \in L$ such that $\sigma(\beta) = \zeta_n \beta$, and we have $L = K(\beta)$.*

As you will show in Exercise 22, Theorem 3.4 is a corollary of the following result from representation theory.

Theorem 3.5. *Let G be a group, let K be a field, and let $\varphi_1, \ldots, \varphi_n : G \to K^*$ be mutually distinct group homomorphisms. Then a K-linear combination*

$$\alpha_1 \varphi_1 + \ldots + \alpha_n \varphi_n = 0 \tag{26}$$

is identically zero if and only if $\alpha_1 = \ldots = \alpha_n = 0$.

Proof. Certainly (26) is zero if all α_i are, so it remains to prove the converse. If $n = 1$, then the statement follows because $\alpha_1 \varphi_1(e) = \alpha_1$ can only be zero if $\alpha_1 = 0$. Now suppose that the statement is shown for at most $n-1$ homomorphisms φ_i. If (26) is identically zero, then certainly we also have

$$0 = \alpha_1 \varphi_1(h) + \ldots + \alpha_n \varphi_n(h) \tag{27}$$

as well as

$$0 = \alpha_1\varphi_1(gh) + \ldots + \alpha_n\varphi_n(gh) = \alpha_1\varphi_1(g)\varphi_1(h) + \ldots + \alpha_n\varphi_n(g)\varphi_n(h). \tag{28}$$

Multiplying the (27) by $\varphi_1(g)$ and subtracting it from (28), we obtain

$$0 = \alpha_2(\varphi_2(g) - \varphi_1(g))\varphi_2(h) + \ldots + \alpha_n(\varphi_n(g) - \varphi_1(g))\varphi_n(h), \tag{29}$$

again for all $h \in G$. By induction, this is only possible if

$$\alpha_2(\varphi_2(g) - \varphi_1(g)) = \ldots = \alpha_n(\varphi_n(g) - \varphi_1(g)) = 0. \tag{30}$$

By mutual distinctness, we can find some $g \in G$ such that $\varphi_1(g) \neq \varphi_2(g)$. Since K is a field, this implies $\alpha_2 = 0$ in light of (30). We have reduced to the case of $n-1$ homomorphisms, so that we are done by induction. ♡

This result in group theory (on the linear independence of so-called characters) clinches the argument via its corollary Theorem 3.5; the fact that σ is of order n combined with ζ_n being in the ground field K implies that the element β constructed in this theorem satisfies

$$\sigma(\beta^n) = (\sigma(\beta))^n = (\zeta_n\beta)^n = \beta^n, \tag{31}$$

so that $\beta^n \in K$ and β can by obtained by means of radicals.

Here are the exercises that serve as a guide to the current theme.

Exercise 19. Prove Theorem 3.3.

Exercise 20. Write algorithms in SageMath that determine the derived series of a finite group G.

Exercise 21. Let $L = K(\beta_1, \ldots, \beta_n)$ be a splitting field of a polynomial $f \in K[x]$, and let $H \subset \mathrm{Gal}(f)$. Show how the fixed field L^H can be determined as the set of solutions of a finite system of linear equations over K. Write algorithms in SageMath that implement this observation.

Exercise 22. Using Theorem 3.5, prove Theorem 3.4. (Hint: Consider the powers of σ as group homomorphisms $L^* \to L^*$ and combine them using n-th roots of unity.)

Exercise 23. Write algorithms in SageMath that given $L|K$ and σ as in Theorem 3.4 determines the element β by solving a finite system of linear equations over K.

Exercise 24. Write algorithms in SageMath that explicitly construct the radicals needed to determine the solution of a cubic equation over $\mathbb{Q}$.

Exercise 25. Derive the Cardano formula VI.(9) using the methods from this section. (Hint: Construct a suitable linear expression in the roots $\beta_1, \beta_2, \beta_3$ of f with coefficients in $\mathbb{Q}(\zeta_3)$ that transforms appropriately under a permutation of the roots β_i.)

Vista

The arithmetic of solvable number fields, such as their ramification and the solution to the associated norm equations, can be studied especially well by means of class field theory, so that in a sense such fields still have a special place in modern mathematics. Already fully understanding the arithmetic of extensions with Galois group D_4 is a very honorable occupation, and it remains relevant in many contexts, for example for the determination of rational points on algebraic curves, as Tim Evink's recent PhD thesis at Ulm University shows.

A complete classification of all abelian Galois extensions of a given field (instead of merely the cyclic ones) is provided by Kummer theory. In turn, this theory can be understood by means of Galois cohomology, a fascinating topic in itself that was already mentioned in Section VI.5 and that contains some of the deepest results on the arithmetic of number fields and their extensions known so far; see [NSW08].

But that, as they say, is a story for another time.

Chapter A

English-German glossary

algebraic	algebraisch
algebraic closure	algebraischer Abschluss
automorphism	Automorphismus
class field theory	Klassenkörpertheorie
cohomology	Kohomologie
conductor	Führer
cyclotomic field	Kreisteilungskörper
decompose	zerfallen
descent	Abstieg
discriminant	Diskriminante
elementary symmetric polynomial	elementarsymmetrisches Polynom
embedding	Einbettung
extend	erweitern
extension	Erweiterung
field extension	Körpererweiterung
finitely generated	endlich erzeugt
fixed field	Fixkörper
fix group	Fixgruppe
function field	Funktionenkörper
Galois (adjective)	galoissch
Galois correspondence	Galoiskorrespondenz
Galois group	Galoisgruppe
group action	Gruppenwirkung
homomorphism	Homomorphismus
inseparable	inseparabel
irreducible	irreduzibel
linear factors	Linearfaktoren
minimal polynomial	Minimalpolynom
monic	normiert
monomial	Monom
number field	Zahlkörper
normal	normal

polynomial	Polynom
polynomial ring	Polynomring
power	Potenz
primitive element theorem	Satz vom primitiven Element
purely inseparable	rein inseparabel
radicals	Radikale
ramification	Verzweigung
ramified	verzweigt
resolvent cubic	kubische Resolvente
(primitive) root of unity	(primitive) Einheitswurzel
separable	separabel
separable closure	separabler Abschluss
simple extension	einfache Erweiterung
solvable (equation)	lösbar
solvable (group)	auflösbar
split	zerfallen
splitting field	Zerfällungskörper
square (noun)	Quadrat
square-free	quadratfrei
subextension	Teilerweiterung
tower law	Turmgesetz
transitive	transitiv
zero	Nullstelle

Bibliography

[Art98] Emil Artin. *Galois theory*. Dover Publications, Mineola, NY, 1998.

[Bar] Arthur Baragar. Constructions using a compass and twice-notched straightedge. *The American Mathematical Monthly*, 109 (2): pp. 151–164, 2002; available online here.

[Dum91] David S. Dummit. Solving solvable quintics. *Math. Comp.*, 57(195):387–401, 1991.

[FK14] Claus Fieker and Jürgen Klüners. Computation of Galois groups of rational polynomials. *LMS J. Comput. Math.*, 17(1):141–158, 2014.

[Gal89] Évariste Galois. *Œuvres mathématiques*. Éditions Jacques Gabay, Sceaux, 1989.

[GR] Alexandre Grothendieck and Michele Raynaud. *Revêtements étales et groupe fondamental (SGA 1)*. arXiv version by Bas Edixhoven et al., 2004.

[Gro95] Alexandre Grothendieck. *La longue marche à travers la théorie de Galois. Tome 1*. Université Montpellier II, Département des Sciences Mathématiques, Montpellier, 1995.

[Har15] Michael Harris. *Mathematics without apologies: Portrait of a problematic vocation*. Princeton University Press, Princeton, NJ, 2015.

[Len] Hendrik W. Lenstra, Jr. *Galois theory for schemes*. Lecture notes, Leiden University, 2008.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024.

[LS00] Hendrik W. Lenstra, Jr. and Peter Stevenhagen. Artin reciprocity and Mersenne primes. *Nieuw Arch. Wiskd. (5)*, 1(1):44–54, 2000.

[Mil22] James S. Milne. *Fields and Galois theory*. Kea Books, Ann Arbor, MI, 2022.

[Neu13] Jürgen Neukirch. *Class field theory*. Springer, Heidelberg, 2013.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, second edition, 2008.

[Rot] Tony Rothman. *Genius and Biographers: The Fictionalization of Evariste Galois*. The American Mathematical Monthly, 89 (2): pp. 84–106, 1982; available online here.

[Ser92] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Darmon.

[SL96] Peter Stevenhagen and Hendrik W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[Sta73] Richard P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.