NOTES ON GALOIS THEORY

Alfonso Gracia-Saz, MAT 347

> *Go to the roots of these calculations! Group the operations. Classify them according to their complexities rather than their appearances! This, I believe, is the mission of future mathematicians. This is the road on which I am embarking in this work.*
>
> *– From the preface to Galois' final manuscript, written the night before he died.*

About these notes

In the fourth and final part of the course we are going to study field extensions and Galois theory. This corresponds to Chapters 13 and 14 in the book. However, the book goes into more depth than we need (and I am also following a different order) so I am providing these notes to help you as a skeleton.

These notes complement, but do not replace, lectures. I am not including proofs and motivation, which we will take care of in class. It is a good exercise to start with these notes and to try and reconstruct all the proofs. You are welcome to follow the book instead (or as well) if you prefer so. In particular, the book contains many extra examples that can be helpful.

If you find any typos or mistakes, please let me know. Parts of these notes are based on a similar handout written by Mira Bernstein (Wellesley College, 2005), with her permission.

Last updated on February 10, 2020 (by Florian Herzig, for the 2018/19 course).

1 Prime subfields and characteristic of a field

This appears in section 13.1 of the book.

Definition 1.1. Let K be a field. The *prime subfield* of K is the smallest subfield of K. Equivalently, it is the intersection of all the subfields of F.

Lemma 1.2. Let K be a field. Let 1_K be its multiplicative identity. For every $n \in \mathbb{Z}$, we can define $n \cdot 1_K \in K$ because $(K, +)$ is an abelian group. Consider the map $\psi : n \in \mathbb{Z} \to n \cdot 1_K \in K$. Then ψ is a ring homomorphism. Moreover, $\ker \psi \trianglelefteq \mathbb{Z}$ is a prime ideal.

Definition 1.3. Under the conditions of Lemma 1.2, let $\ker \psi = (n) = \mathbb{Z}n$ where $n \in \mathbb{Z}$ is either a positive prime number or zero. Then we say that the *characteristic* of K is n. We write $\operatorname{char} K = n$.

Proposition 1.4. Let K be a field. If $\operatorname{char} K = p$ is a prime, then the prime subfield of K is $\mathbb{F}_p$. If $\operatorname{char} K = 0$, then the prime subfield of K is $\mathbb{Q}$.

Hint: Apply the first isomorphism theorem to ψ. If $\operatorname{char} K = 0$, remember that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

Lemma 1.5. If $\operatorname{char} K = p$ is prime, then $p \cdot a = 0$ for every $a \in K$.

Examples 1.6. What is the characteristic of $\mathbb{C}$? Find an example of an infinite field with characteristic prime.

2 Field extensions

This appears in sections 13.1–13.2 of the book.

2.1 Definitions

Definition 2.1. A *field extension* is a field homomorphism $i : F \to K$, where F and K are fields.

Notice that every such homomorphism is necessarily injective. (The kernel is an ideal, and we require $i(1_F) = 1_K$, so i cannot be the zero map.)

Examples 2.2. The inclusion maps $i_1 : \mathbb{Q} \to \mathbb{C}$ and $i_2 : F \to F(X)$ (where F is any field and X is a formal variable) are field extensions.

Remark 2.3. If $i : F \to K$ is a field extension, we often identify F with its image $i(F)$. Thus we think of F as a subfield of K and i as the inclusion (identity) map. In this case we say that K is an extension of F, and use the notation K/F for the extension. Whenever there is no ambiguity, we will use these two points of view (field homomorphism vs subfield) interchangeably.

For the rest of this section, let K/F be a field extension.

Definition 2.4. Suppose $a_1, \ldots, a_n \in K$. The smallest subring of K containing both F and all the a_i's is denoted $F[a_1, \ldots, a_n]$. It is called the *subring of K generated by $a_1, \ldots, a_n$ over F.*

The smallest subfield of K containing both F and all the a_i's is denoted $F(a_1, \ldots, a_n)$. It is called the *subfield of K generated by $a_1, \ldots, a_n$ over F.*

Proposition 2.5. $F(a_1, \ldots, a_n)$ is the field of fractions of $F[a_1, \ldots, a_n]$.

Examples 2.6.

(i) In $\mathbb{C}$, $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$.

(ii) In $\mathbb{R}$, $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$.

(iii) In $\mathbb{R}$, $\mathbb{Q}[\sqrt[3]{5}] \neq \{a + b\sqrt[3]{5} : a, b \in \mathbb{Q}\}$. Any idea what it might be instead? How about $\mathbb{Q}(\sqrt[3]{5})$?

(iv) In $\mathbb{R}$, $\mathbb{Q}(i + \sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$.

Remark 2.7. The ring of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in F is denoted $F[x_1, \ldots, x_n]$. Its field of fractions (rational expressions in $x_1, \ldots, x_n$) is denoted $F(x_1, \ldots, x_n)$.

The similarity of this notation to Definition 2.4 is intentional and consistent, since

$$F[a_1, \ldots, a_n] \;=\; \{f(a_1, \ldots, a_n) :\; f \in F[x_1, \ldots, x_n]\},$$

and $F(a_1, a_2, \ldots)$ is the field of fractions of $F[a_1, \ldots, a_n]$.

In other words, $F[a_1, \ldots, a_n]$ consists precisely of all polynomial combinations of the a_i's, while $F(a_1, \ldots, a_n)$ consists of quotients of such polynomial combinations. However, as we saw in Example 2.6, there are often simpler ways of characterizing the elements of $F(a_1, \ldots, a_n)$ and $F[a_1, \ldots, a_n]$, since different polynomials and rational expressions in $a_1, \ldots a_n$ can simplify and evaluate to the same element in K.

Definition 2.8. If there exists $\alpha \in K$ such that $K = F(\alpha)$, then K/F is called a *simple* extension.

Definition 2.9. An element $\alpha \in K$ is said to be *algebraic over* F if α is the root of some nonzero polynomial in $F[X]$; otherwise, α is said to be *transcendental over* F. Real or complex numbers that are algebraic (resp. transcendental) over $\mathbb{Q}$ are called simply algebraic (resp. transcendental) numbers. The field extension K/F is called *algebraic* when α is algebraic over F for every $\alpha \in K$.

Examples 2.10.

(i) For all $k, n \in \mathbb{N}$, $\sqrt[n]{k}$ is algebraic, since it is the root of $X^n - k$.

(ii) The field extension $\mathbb{C}/\mathbb{R}$ is algebraic. Given $\alpha = a + bi \in \mathbb{C}$, we see that α is a root of $(X - a)^2 + b^2$.

Remark 2.11. The set of algebraic numbers (over $\mathbb{Q}$) is countable. (Why?) Since we know that $\mathbb{R}$ is uncountable, it follows that "most" real numbers are transcendental. However, explicit examples of numbers transcendental over $\mathbb{Q}$ are very hard to find, since it is difficult to prove that a given number is not the root of *any* polynomial. It was shown in the 19th century that both e and π are transcendental over $\mathbb{Q}$.

2.2 Simple extensions

We continue assuming that K/F is a field extension.

Proposition 2.12. Let $\alpha \in K$. Consider the evaluation map $E_\alpha : f(X) \in F[X] \to f(\alpha) \in K$. Then E_α is a ring homomorphism with image $F[\alpha]$. Moreover, $\ker E_\alpha \trianglelefteq F[X]$ is a prime ideal.

Theorem 2.13. Continue with the notation of Proposition 2.12. The map E_α is injective iff $\alpha \in K$ is transcendental over F. In that case, $F[\alpha] \cong F[X]$ and $F(\alpha) \cong F(X)$. In particular, $F[\alpha] \neq F(\alpha)$.

Definition 2.14. Let $\alpha \in K$ be algebraic over F. Let $I = \ker E_\alpha$ as in Proposition 2.12. Since $F[X]$ is a PID, we know that I is principal. Since $I \neq 0$, we know that $I = (f(X))$ for a unique monic polynomial $f(X) \in F(X)$. Moreover, since I is prime, we know that $f(X)$ is irreducible. We say that $f(X)$ is the *minimal polynomial of α over F* and we denote it by $m_{\alpha,F}(X) := f(X)$.

Lemma 2.15. Let $\alpha \in K$ be algebraic. Let $g(X) \in F[X]$. Then α is a root of $g(X)$ if and only if $m_{\alpha,F}(X)$ divides $g(X)$.

Lemma 2.16. Let $\alpha \in K$ be algebraic. Let $g(X) \in F[X]$. Assume that α is a root of $g(X)$. TFAE:

- $g(X)$ is the minimal polynomial of α over F.
- $g(X)$ is monic and irreducible.
- $g(X)$ is monic and it has the smallest degree among non-zero polynomials that have α as a root.

Examples 2.17. Both i and $\sqrt{2}$ are algebraic over $\mathbb{Q}$ and over $\mathbb{R}$. Over $\mathbb{Q}$ they both have degree 2, with minimal polynomials $x^2 + 1$ and $x^2 - 2$ respectively. Over $\mathbb{R}$, i still has degree 2, but $\sqrt{2}$ has degree 1, with minimal polynomial $x - \sqrt{2}$.

Proposition 2.18. An element $\alpha \in K$ has degree 1 over F if and only if $\alpha \in F$.

Exercise 2.19. What complex numbers have degree ≤ 2 over $\mathbb{Q}$? over $\mathbb{R}$?

Theorem 2.20. Suppose $\alpha \in K$ is algebraic, with minimal polynomial $f(X)$ over F. Then

$$F(\alpha) \;=\; F[\alpha] \;\cong\; F[X]/(f(X)).$$

Example 2.21. $\mathbb{R}[X]/(X^2+1) \cong \mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$.

Example 2.22. In $\mathbb{R}$, $\mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} : a, b, c \in \mathbb{Q}\}$. We don't have an algorithm for finding inverses in this field yet, but we know that they are guaranteed to exist. Find an algorithm for finding inverses in this field.

Exercise 2.23. More generally, let $f(X) \in F[X]$ be irreducible and monic. Find an algorithm for finding inverses in the field $F[X]/(f(x))$.

Corollary 2.24. Suppose α_1 and α_2 have the same minimal polynomial $f(X)$ over F. Then $F(\alpha_1) \cong F(\alpha_2)$, since both are isomorphic to $F[X]/(f(X))$. This is true even if α_1 and α_2 come from different extensions of F (i.e. different fields).

Remark 2.25. The interpretation of Corollary 2.24 is that different roots of the same irreducible polynomial in $F[X]$ are indistinguishable from the perspective of F. For example, i and $-i$ are indistinguishable from the perspective of $\mathbb{R}$.

Example 2.26. Let $\omega = \frac{i\sqrt{3}-1}{2}$.

(i) ω is a cube root of 1. (Either verify directly that $w^3 = 1$ or, better, plot ω in the complex plane and argue geometrically.)

(ii) $\mathbb{Q}(\sqrt[3]{5}) \neq \mathbb{Q}(\omega\sqrt[3]{5})$, but $\mathbb{Q}(\sqrt[3]{5}) \cong \mathbb{Q}(\omega\sqrt[3]{5})$.

Theorem 2.27. Let $f(X) \in F[X]$ be any non-constant polynomial. Then there exists an extension K/F such that $f(X)$ has a root in K.

[The proof is almost trivial, yet confusing at first because of its abstract nature. *Hint:* Assume first that f is irreducible, then take $K := F[T]/(f(T))$, where T is a new formal variable.]

Remark 2.28. Theorem 2.27 is an extremely important theorem! The construction of K seems (and is) artificial, but that doesn't matter. The theorem says that given any polynomial f over a field F, if we want to think of f as having a root, we can – not necessarily in F, but in *some* larger field. We now have a rigorous justification for those 16th century mathematicians who first "imagined" $\sqrt{-1}$. They simply decided to assume that X^2+1 has a root *somewhere*, even if not in $\mathbb{R}$. For centuries people worried that such an assumption was invalid – that i somehow wasn't "real". Theorem 2.27 tells us exactly where the polynomial X^2+1 has a root: in the field $\mathbb{R}[T]/(T^2+1)$, which we happen to call $\mathbb{C}$. Corollary 2.24 tells us that this is the "only" place where X^2+1 has a root.

Remark 2.29. Just because an irreducible polynomial $f(X) \in F[X]$ has a root α in some extension K/F, it doesn't follow that $K \simeq F[X]/(f(X))$. K could be a lot bigger than just $F(\alpha)$. Find an example of that situation.

Remark 2.30. We have shown that every simple extension of F is isomorphic either to $F(X)$ or to $F[X]/(f(X))$ for some irreducible monic polynomial in $F[X]$. We have also seen (part (iii) of Example 2.6) that it may not be obvious at first glance whether a given extension is simple or not.

Examples 2.31. Read examples from pages 515, 516, and 521 in the book.

Theorem 2.32. ["Theorem A" – Very important!] Let K/F and K'/F' be field extensions, and suppose $\varphi : F \to F'$ is an isomorphism. Let $\widetilde{\varphi}$ be the natural map from $F[X]$ to $F'[X]$ that extends φ. Suppose $\alpha \in K$ is a root of an irreducible polynomial $f(X) \in F[X]$ and $\beta \in K'$ is a root of $\widetilde{\varphi}(f) \in F'[x]$. Then there is an isomorphism

$$\psi : F(\alpha) \to F'(\beta)$$

such that $\psi(a) = \varphi(a)$ for all $a \in F$ and $\psi(\alpha) = \beta$.

[*Hint:* Once you figure out what this theorem is saying, it seems pretty obviously true – though you still have to take care of some important details, such as the fact that $\widetilde{\varphi}(f)$ is irreducible. The cleanest way to define the isomorphism ψ is to consider the composition of $\widetilde{\varphi}$ with the canonical map $F'[x] \to F'[x]/(\widetilde{\varphi}(f(X)))$ and then find the kernel of this composition. This is more abstract then trying to define ψ directly between $F(\alpha)$ and $F'(\beta)$, but it will save you a lot of "handwaving" arguments.]

Corollary 2.33. Let K/F be a field extension. Let $\alpha, \beta \in K$ such that $m_{\alpha,F}(X) = m_{\beta,F}(X)$. Then there is an isomorphism

$$\psi : F(\alpha) \to F(\beta)$$

such that $\psi(a) = a$ for all $a \in F$ and $\psi(\alpha) = \beta$. (This corollary is obviously a particular case of Theorem 2.32, but it is one that we will use frequently.)

2.3 The degree of an extension

We continue assuming that K/F is a field extension.

Consider the question: If α and β are algebraic over F, is $\alpha + \beta$ algebraic over F? Our intuition says that this is probably true, but try to prove it directly! It is not apparent how the proof could work.

Definition 2.34. Since elements of K can be added and multiplied by elements of F, K is automatically a vector space over F. (All the vector space axioms are just special cases of the field axioms.) The dimension of K as a vector space over F (which could be ∞) is called the *degree of the extension*, written $[K : F]$. If $[K : F]$ is finite, we say that $K : F$ is a *finite extension*; otherwise, we say it is an *infinite extension*.

Given $\alpha \in K$, we say that the *degree of α over F* is $[F(\alpha) : F]$.

Exercise 2.35. Find the degrees of the following extensions:

(i) $\mathbb{C}/\mathbb{R}$

(ii) $\mathbb{Q}(X)/\mathbb{Q}$

(iii) $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$

(iv) K/F, where $K = F[X]/(f(X))$ and $f(X) \in F[X]$ is irreducible.

Proposition 2.36. If F is a finite field and $[K : F]$ is finite, how are the orders of K and F related?

Theorem 2.37. Let $\alpha \in K$.

- If α is transcendental over F, then $[F(\alpha) : F] = \infty$.
- If α is algebraic over F, then $[F(\alpha) : F] = \deg m_{\alpha,F}(X)$.

In particular, α is algebraic over F if and only if $[F(\alpha) : F]$ is finite.

Exercise 2.38. Let F be a field with characteristic not 2. Describe all field extensions of F with degree 2.

Theorem 2.39 (Tower Law)**.** Let L/K and K/F be field extensions. Then $[L : F] = [L : K][K : F]$. Here we adopt the convention that $n \cdot \infty = \infty \cdot \infty = \infty$ for any $n \in \mathbb{N}$.

In particular, given a basis for L as a K-vector space, and a basis for K as an F-vector space, can you write a basis for L as an F-vector space? This particular construction will be useful later.

Exercise 2.40. Suppose $\alpha \in K$ has odd degree over F. Prove that $F(\alpha^2) = F(\alpha)$. What if α has even degree over F?

Lemma 2.41. Let L/K and K/F be field extensions, $\alpha \in L$. How are $m_{\alpha,K}(X)$ and $m_{\alpha,F}(X)$ related?

Lemma 2.42. Let $\alpha_1, \ldots, \alpha_n \in K$. Suppose we adjoin the α's to F one at a time:

$$F_0 = F, \quad F_1 = F_0(\alpha_1), \quad F_2 = F_1(\alpha_2), \quad \ldots, \quad F_n = F_{n-1}(\alpha_n).$$

Then the result is the same as adjoining all the α's at once:

$$F_n = F(\alpha_1, \ldots, \alpha_n).$$

In other words, we can view any extension of the form $F(\alpha_1, \ldots, \alpha_n)$ as a "tower" of simple extensions:

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2) \cdots (\alpha_i).$$

Theorem 2.43. If $\alpha_1, \ldots, \alpha_n \in K$ are algebraic over F, with degrees $d_1, \ldots, d_n$, then $[F(\alpha_1, \ldots, \alpha_n) : F]$ is a finite extension of degree at most $d_1 \cdots d_n$.

Exercise 2.44.

(i) What is the degree of $\mathbb{Q}(i, \sqrt{5})$ as an extension of $\mathbb{Q}$? What does a typical element of this extension look like?

(ii) What is $m_{i+\sqrt{5},\mathbb{Q}(i)}(X)$?

(iii) Based on Example 2.6(iv), what is the degree of $m_{i+\sqrt{5},\mathbb{Q}}(X)$? Find this polynomial. What are its other roots in $\mathbb{C}$?

Definition 2.45. Let K_1 and K_2 be subfields of K. Then the *composite* of K_1 and K_2, denoted K_1K_2 is the smallest subfield of K that contains both K_1 and K_2.

Example 2.46. What is the composite of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$?

Lemma 2.47. Let K/F be a field extension. Let K_1 and K_2 be subfields of K such that K_1/F and K_2/F are finite field extensions. Then $[K_1K_2 : K_1] \leq [K_2 : F]$ (draw a picture of the extensions!).

Note that this lemma implies $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$.

Theorem 2.48. The following are equivalent:

- The field extension K/F is algebraic (i.e., α is algebraic over F for every $\alpha \in K$) and finitely generated (i.e., there exists $\alpha_1, \ldots, \alpha_n \in K$ such that $K = F(\alpha_1, \ldots, \alpha_n)$).
- The field extension K/F is generated by finitely-many algebraic elements (i.e., there exists $\alpha_1, \ldots, \alpha_n \in K$ algebraic over F such that $K = F(\alpha_1, \ldots, \alpha_n)$).
- The field extension K/F is finite (i.e., $[K : F] < \infty$).

Theorem 2.49. Let L/K and K/F be algebraic field extensions. Then L/F is an algebraic field extension.

(Suggestion: Let $\alpha \in M$. Let $m_{\alpha,K}(X) = \beta_m X^m + \cdots + \beta_0$. Define $L = F(\beta_0, \ldots, \beta_m)$. Notice that $L(\alpha)/L$ and L/F are both finite.)

Corollary 2.50. Let K/F be a field extension. Define

$$K_{alg} := \{\alpha \in K \mid \alpha \text{ is algebraic over } F\}$$

Then K_{alg} is a field.

Example 2.51. Let $\mathbb{A} \subseteq \mathbb{C}$ be the set of all algebraic numbers over $\mathbb{Q}$. Then $\mathbb{A}/\mathbb{Q}$ is a field extension that is algebraic but not finite.

3 Constructions with straightedge and compass

3.1 General constructions

For centuries, mathematicians searched for methods to solve geometric constructions using only straightedge and compass. It never occurred to the ancient Greeks that some of these constructions were impossible.

Definition 3.1. Let P_0 be a set of points in the Euclidean plane $\mathbb{R}^2 = \mathbb{C}$. The two basic constructions are

Operation 1 (straightedge): draw a line through any two points of P_0.

Operation 2 (compass): draw a circle centered at any point of P_0 and with radius equal to the distance between a pair of points in P_0.

The points of intersection of any lines and circles drawn using Operations 1 and 2 are said to be *constructible from P_0 in one step*. Given $r \in \mathbb{R}^2$, we say that r is *constructible from P_0* if there exist points $r_1, r_2, \ldots, r_n = r$ such that r_i is constructible in one step from

$$P_0 \cup \{r_1, \ldots, r_{i-1}\}$$

for $i = 1, \ldots, n$.

Example 3.2. Using Operations 1 and 2 we can do the following constructions:

(i) Bisect a given segment.

(ii) Draw the bisector of a given angle.

(iii) Given a line l and a point P, draw a line through P perpendicular to l

(iv) Given a line l and a point P, draw a line through P parallel to l.

Lemma 3.3. Let $z \in \mathbb{C}$. The following are equivalent:

(i) z can be constructed from $\{0, 1\}$.

(ii) We can construct segments with length $\operatorname{Re} z$ and $\operatorname{Im} z$ starting from a single segment of length 1 by using operations 1 and 2.

Definition 3.4. We denote by Δ_2 the set of all $z \in \mathbb{C}$ that satisfy the equivalent conditions of Lemma 3.3.

Exercise 3.5. Here are three classical construction problems. Translate each one of them into a statement of the form "$z \in \Delta_2$" or " the point z can be constructed from the set of points P_0".

(i) Squaring the circle: given a circle, construct a square that has the same area.

(ii) Doubling the cube: given a cube, construct a cube with volume twice as large.

(iii) Trisecting an arbitrary angle.

Theorem 3.6. Δ_2 is a subfield of $\mathbb{C}$ and $\mathbb{Q}(i) \subseteq \Delta_2$.

Lemma 3.7. Let F be a field with $\mathbb{Q}(i) \subseteq F \subseteq \mathbb{C}$ such that $\overline{F} = F$, where $\overline{F} = \{\overline{z} : z \in F\}$. Let $z \in \mathbb{C}$. Assume that z can be constructed from a set of points in F in just one step. Prove that $[F(z) : F] = 1$ or 2 and that $\overline{F(z)} = F(z)$.

[*Hint:* First show that $z \in F$ iff both $\operatorname{Re} z$ and $\operatorname{Im} z$ are in F. Then you can use equations for lines and circles in $\mathbb{R}^2$.]

Proposition 3.8. Let K/F be a field extension with characteristic not equal to 2. Then the following are equivalent:

(i) $[K : F] = 2$.

(ii) There exists $\alpha \in K$ such that $K = F(\alpha)$, $\alpha \notin F$, $\alpha^2 \in F$.

We sometimes abbreviate this by saying that $K = F(\sqrt{D})$ for some $D \in F$. (Why?)

Theorem 3.9. Let $z \in \mathbb{C}$. Then the following are equivalent:

(i) $z \in \Delta_2$.

(ii) There exist fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ such that $z \in F_n$ and $[F_i : F_{i-1}] = 2$ for every i.

Corollary 3.10. Let $z \in \mathbb{C}$. If $z \in \Delta_2$ then $[\mathbb{Q}(z) : \mathbb{Q}] = \deg m_{z,\mathbb{Q}}(X)$ is a power of 2.

Corollary 3.11.

(i) It is impossible to square the circle.

(ii) It is impossible to double the cube.

(iii) It is impossible to trisect an arbitrary angle.

3.2 Construction of regular polygons

Definition 3.12. We denote by $\mathcal{P}$ the set of integers $n \geq 2$ such that a regular n-gon is constructible with Operations 1 and 2.

Example 3.13. $2, 3, 4, 6 \in \mathcal{P}$.

Proposition 3.14.

(i) If a divides b and $b \in \mathcal{P}$, then $a \in \mathcal{P}$.

(ii) Let n be a positive integer. Then

$$a \in \mathcal{P} \iff 2^n a \in \mathcal{P}.$$

(iii) Let a, b be two coprime integers.

$$(a \in \mathcal{P} \text{ and } b \in \mathcal{P}) \iff ab \in \mathcal{P}$$

Suggestion: Use Bezout identity.

Note 3.15. Thanks to Proposition 3.14, we only need to consider whether regular p^n-gons are constructible, for p an odd prime and n an integer.

Definition 3.16. An *n-th root of unity* is a complex number[1] z which is a root of the polynomial $z^n - 1$. A *primitive n-th root of unity* is an n-th root of unity which is not an m-th root of unity for any $m < n$. There are exactly n distinct n-th roots of unity and $\varphi(n)$ distinct primitive n-th roots of unity for any positive integer n, where φ is the Euler function.

We will denote

$$\zeta_n := e^{2\pi i/n}.$$

The n-th roots of unity are

$$\{\zeta_n^m : 0 \leq m \leq n-1\}.$$

The primitive n-th roots of unity are

$$\{\zeta_n^m : 0 < m < n, n \text{ and } m \text{ are coprime}\}.$$

Note that in some other contexts, notation is abused and we may read simply "*the* n-th root of unity" to mean ζ_n.

Lemma 3.17. Let $n \geq 2$ be a positive integer. The following are equivalent:

- $n \in \mathcal{P}$.
- $\zeta_n \in \Delta_2$.

Corollary 3.18. Let $p \in \mathbb{Z}$ be a prime. If a regular p-gon is constructible, then $p - 1$ is a power of 2.

Hint: What is $m_{\zeta_p,\mathbb{Q}}(X)$?

Example 3.19. Prove that a regular pentagon is constructible, i.e. that $5 \in \mathcal{P}$. Note that you need to prove that your construction method works, and not only to give an algorithm.

Suggestion: Here is one, among many methods. Consider the points in the plane $z_j = (\cos \frac{2\pi j}{5}, \sin \frac{2\pi j}{5})$ for $j = 0, \ldots, 4$. Prove that $z_0 + z_1 + z_2 + z_3 + z_4 = 0$. (You can do that either by rotational invariance, or using complex numbers and the formula for the sum of a geometric sequence.) Define a to be the x-coordinate of $z_1 + z_4$ and b to be the x-coordinate of $z_2 + z_3$. (What are a and b actually?) Try to calculate $a + b$ and ab using the expression you just proved (you will need ingenuity, complex numbers, or heavy trigonometry). Write down an quadratic equation having a and b as roots, who turn out to be old friends. What is left?

Joke 3.20. What did the logarithm of the sixteenth root of unity say after all the pie was gone?

[1] We can talk about roots of unity in more general extensions than $\mathbb{C}/\mathbb{Q}$, but for now this will be enough.

4 Introduction to Galois theory

4.1 The Galois group

In this section, F always denotes a field and K/F a field extension. We are going to construct a group from each field extension. Our goal is to be able to obtain information about the field extension by studying this group.

Definition 4.1. An *automorphism* of a field K is an isomorphism from K to itself. We denote by $\mathrm{Aut}(K)$ the set of all such automorphisms.

If K/F is a field extension, then an *F-automorphism of K* (also called an *automorphism of K over F*) is an automorphism φ of K which leaves every element of F fixed. In other words, $\varphi(a) = a$ for all $a \in F$; equivalently, $\varphi|_F = \mathrm{id}$.

Example 4.2. Complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$. It is also a $\mathbb{Q}$-automorphism of $\mathbb{C}$.

Lemma 4.3. The set of F-automorphisms of K forms a group (under composition).

Definition 4.4. The group of F-automorphisms of K is called the *Galois group of K over F*, denoted $\mathrm{Gal}(K/F)$.

Exercise 4.5. If F is the prime subfield of K, then $\mathrm{Aut}(K) = \mathrm{Gal}(K/F)$.

Proposition 4.6. Let $\varphi \in \mathrm{Gal}(K/F)$.

(i) If $f(x) \in F[x]$ and $\alpha \in K$ is a root of $f(x)$, then so is $\varphi(\alpha)$.

(ii) For every $\alpha \in K$, α and $\varphi(\alpha)$ are either both transcendental or have the same minimal polynomial (hence the same degree) over F.

(iii) Given $f(x) \in F[x]$, there is an action of $\mathrm{Gal}(K/F)$ on the set of roots of $f(x)$ in K. (This is an immediate consequence of the previous points once you figure out what it is saying.)

Proposition 4.7. Suppose $K = F(\alpha_1, \ldots, \alpha_n)$ and $\varphi, \varphi' \in \mathrm{Gal}(K/F)$. If $\varphi(\alpha_i) = \varphi'(\alpha_i)$ for all i then $\varphi = \varphi'$. In other words, an F-automorphism of $F(\alpha_1, \ldots, \alpha_n)$ is uniquely determined by what it does to $\alpha_1, \ldots, \alpha_n$.

Proposition 4.8. Suppose $K = F(\alpha)$ for some $\alpha \in K$, and α has minimal polynomial $f(x)$ over F. Then $|\mathrm{Gal}(K/F)|$ = number of roots of $f(x)$ in K. (*Hint:* use "Theorem A".)

Examples 4.9. Find $\mathrm{Gal}(K/F)$ in each case: list all the elements and identify the group structure. Part (iii) requires a bit more work. You can solve part (iv) already (it is a very good exercise) but I will postpone it till later.

(i) $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}$ is not a perfect square in $\mathbb{Q}$.

(ii) $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{d})$, where $d \in \mathbb{Q}$ is not a perfect cube in $\mathbb{Q}$.

(iii) $F = \mathbb{Q},\ K = \mathbb{Q}(i, \sqrt{5})$.

(iv) $F = \mathbb{Q},\ K = \mathbb{Q}(\zeta_n)$, where $\zeta_n := e^{2\pi i/n}$.

4.2 The Galois correspondence

Definition 4.10. Let H be a subgroup of $\mathrm{Gal}(K/F)$. The *fixed field of* H, denoted $\mathrm{Inv}(H)$ or $\widehat{I}(H)$, consists of all the elements of K that are fixed by all the automorphisms in H. In other words,

$$\widehat{I}(H) = \{\alpha \in K : \varphi(\alpha) = \alpha \text{ for all } \varphi \in H\}.$$

Proposition 4.11. $\widehat{I}(H)/F$ is a field extension (i.e. $\widehat{I}(H)$ really is a field —so we were justified in calling it the fixed field of H—, and it contains F).

Proposition 4.12. If $H_1 \leq H_2$ are subgroups of $\mathrm{Gal}(K/F)$, how are $\widehat{I}(H_1)$ and $\widehat{I}(H_2)$ related?

Examples 4.13. List all the subgroups of $\mathrm{Gal}(K/F)$ for Example 4.9, parts (i), (ii), (iii), and find the corresponding fixed fields. (Only part (iii) is actually interesting.)

Definition 4.14. If M is a field such that $F \subseteq M \subseteq K$, we call M an *intermediate* field between F and K. We denote $\mathrm{Gal}(K/M)$ by $\widehat{G}(M)$.

Proposition 4.15. $\widehat{G}(M)$ is a subgroup of $\mathrm{Gal}(K/F)$.

Proposition 4.16. If $M_1 \subseteq M_2$ are intermediate fields, how are $\widehat{G}(M_1)$ and $\widehat{G}(M_2)$ related?

Example 4.17. Find all the intermediate fields between F and K for Examples 4.9, parts (i), (ii), (iii). For each intermediate field M, find $\widehat{G}(M)$. Be sure to prove that, in each case, there are no other intermediate fields. (Again, only part (iii) is really interesting, and it actually takes some work.)

Proposition 4.18. Note that we have defined two functions:

$$\begin{aligned} \widehat{I} &: \{\text{subgroups of } \mathrm{Gal}(K/F)\} \longrightarrow \{\text{intermediate fields between } F \text{ and } K\} \\ \widehat{G} &: \{\text{intermediate fields between } F \text{ and } K\} \longrightarrow \{\text{subgroups of } \mathrm{Gal}(K/F)\}. \end{aligned}$$

Unfortunately, these functions are not quite inverses of each other:

(i) For any intermediate field M between F and K, how are M and $\widehat{I}(\widehat{G}(M))$ related? Find an example (among ones we've seen so far) where they are not equal.

(ii) For any subgroup H of $\mathrm{Gal}(K/F)$, how are H and $\widehat{G}(\widehat{I}(H))$ related? For an example where they are not equal, see the homework.

(iii) Find some examples (among ones we've seen so far) where the functions $\widehat{G}$ and $\widehat{I}$ actually *are* inverses.

Remark 4.19. When the functions $\widehat{G}$ and $\widehat{I}$ *are* inverses of each other, they establish an inclusion-reversing (see Propositions 4.12 and 4.16) one-to-one correspondence between subgroups of $\mathrm{Gal}(K/F)$ and intermediate fields. This will allow us to understand the structure of a field extension by analyzing the structure of its Galois group —*cough* functors *cough*. This correspondence is called the *Galois correspondence*.

Eventually, we would like to understand under what circumstances such a correspondence is guaranteed to exist.

Remark 4.20. How is this going to help us?

Remember what we have proven about constructibility of regular polygons with straightedge and compass. We showed that a regular n-gon is constructible if and only if there is a 2-filtered field extension $K/\mathbb{Q}(i)$ such that $\zeta_n \in K$. An extension K/F is 2-filtered when there are subextensions $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ such that $[K_i : K_{i-1}] = 2$ for all i. If we manage to show that $\widehat{G}$ and $\widehat{I}$ are inverses of each other, we can translate the condition "the field extension is 2-filtered" into a condition about its Galois group. Then we will use all the group theory we know to solve the problem.

Discussion 4.21. What may go wrong?

In general, $\widehat{G}$ and $\widehat{I}$ are not inverses of each other when "there are not enough elements in the Galois group". Consider an element $\alpha \in K$. We know that $\mathrm{Gal}(K/F)$ acts on the set of roots of $m_{\alpha,F}(X)$. The problem is that $m_{\alpha,F}(X)$ may not have enough roots in K. Two things may go wrong:

- $m_{\alpha,F}(X)$ may not have all of its roots in K (you have already seen an example of this). Then the Galois group is "too small". We will avoid this by imposing that our field extensions are *normal*.
- $m_{\alpha,F}(X)$ may have all of its roots in K, but there may be repeated roots. Think about this: a polynomial with coefficients in F, which is irreducible in F, which has all of its roots in some extension field K, and which has some repeated root in K. This is crazy! I challenge you to come up with such a example without reading ahead. Anyway, this may happen and in this case the Galois group is also "too small". We will avoid this by imposing that our field extensions are *separable*.

5 Splitting fields and normal extensions

5.1 Splitting fields

Definition 5.1. Let K/F be a field extension and let $f(X) \in F[X]$. We say that $f(X)$ splits in K if it can be written as product of degree-1 polynomials with coefficients in K.

Example 5.2. Over which of the following fields does the polynomial X^2+1 split? $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{F}_2$, $\mathbb{F}_3$.

Lemma 5.3. Let K/F be a field extension. Let $f(X) \in F[X]$ and assume that $f(X)$ splits in K:

$$f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$$

for $c \in F^\times$; $\alpha_1, \ldots, \alpha_n \in K$. Then TFAE:

- $K = F(\alpha_1, \ldots, \alpha_n)$.
- If M is a field, $F \subseteq M \subseteq K$ and $f(X)$ splits in M, then $M = K$. (In other words, K is a minimal field extension of F among those where $f(X)$ splits.)

Definition 5.4. A field K satisfying the equivalent conditions in the previous lemma is called a *splitting field* of $f(X)$ over F.

Remark 5.5. If K/F is a field extension and $f(X) \in F[X]$ splits in K, then K *contains* a splitting field of $f(X)$ over F.

Examples 5.6. For each one of the following polynomials in $\mathbb{Q}[X]$, describe their splitting fields over $\mathbb{Q}$ and compute the degree of the field extension.

(i) $X^2 - 2$

(ii) $X^4 - X^2 - 2$.

(iii) $X^3 - 2$.

(iv) $X^n - 1$.

(v) $X^n - 2$. (You cannot compute the degree of this extension exactly for arbitrary n, but you can do it when n is prime.)

(vi) $X^8 - 2$.

Theorem 5.7. Let $f(X) \in F[X]$ be a polynomial with degree n. Then there exist a splitting field K of $f(X)$ over F and $[K:F] \leq n!$.

Theorem 5.8 ("Theorem B" – Very important!)**.** Let $\varphi : F_1 \to F_2$ be a field isomorphism. Let $\tilde{\varphi} : F_1[X] \to F_2[X]$ be the ring isomorphism that φ induces over the rings of polynomials. Let $f_1 \in F_1[X]$ and let $f_2(X) := \tilde{\varphi}(f_1(X))$. Let E_i be a splitting field of $f_i(X)$ over F_i.

Then there exist a field isomorphism $\sigma : E_1 \to E_2$ such that $\sigma|_{F_1} = \varphi$.

Remark 5.9. Compare Theorem A (2.32) and Theorem B (5.8).

Corollary 5.10. The splitting field of a polynomial is unique up to isomorphism.

5.2 Normal extensions and normal closure

Theorem 5.11. Let K/F be a finite field extension. Then the following are equivalent:

(i) K is the splitting field of some (non-necessarily irreducible) polynomial in $F[X]$.

(ii) For any field $E \supseteq K$ and any F-homomorphism $\varphi : K \to E$, $\varphi(K) \subseteq K$.

(iii) For any field $E \supseteq K$ and any F-homomorphism $\varphi : K \to E$, $\varphi(K) = K$.

(iv) If $f(X) \in F[X]$ is an irreducible polynomial and it has a root in K, then $f(X)$ splits in K.

(v) For every $\alpha \in K$, the minimal polynomial of α over F splits in K.

(vi) $K = F(\alpha_1, \ldots, \alpha_n)$ and the minimal polynomial of α_j over F splits in K for all $j = 1, \ldots, n$.

[*Notes:* You may want to use Theorems A and B.

Notice that these characterizations have different "roles". On a given example, it will be easy for us to check that condition (i) or (vi) are satisfied, and we will want to use that condition (iv) or (v) are true. Conditions (ii) and (iii) are convenient as lemmata for theoretical proofs.]

Definition 5.12. A field extension satisfying the equivalent conditions in the previous theorem is called a *normal extension*.

Definition 5.13. Let $F \subseteq K \subseteq N$ be fields. The extension N/F is called a *normal closure* of K/F when

- N/F is normal,
- If M is a field, $K \subseteq M \subseteq N$, and M/F is normal, then $M = N$. (In other words, N/F is a minimal normal extension of F containing K.)

Proposition 5.14. Let K/F be a finite field extension. Assume that $K = F(\alpha_1, \ldots, \alpha_n)$. Let

$$f(X) = \prod_{j=1}^{n} m_{\alpha_j, F}(X).$$

Then a normal closure of K/F is the same thing as a splitting field of $f(X)$ over K. In particular, normal closures exist and are unique up to isomorphism.

Example 5.15. What are the normal closures of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$?

Proposition 5.16. Let K/F be a finite field extension and let N/F be its normal closure. Then there are fields $K_1, \ldots K_r$ for some finite number r such that

- $F \subseteq K_i \subseteq N$,

- $N = K_1K_2\cdots K_r$ (i.e. N is the composite of $K_1, \ldots, K_r$ — see Definition 2.45),
- there is a field isomorphism between K_i and K which fixes F, for all i.

This means that the normal closure of K/F is the composite of finitely many field extensions isomorphic to K/F.

[*Hint:* Write $K = F(\alpha_1, \ldots, \alpha_n)$. Let $f(X)$ be defined as in Proposition 5.14. Let β be a root of $m_{\alpha_i,F}(X)$. Use Theorems A and B to prove that there is some F-automorphism φ of N such that $\varphi(\alpha_i) = \beta$. Let $L_\beta := \varphi(K)$. Then N is the composite of the fields in the set $\{L_\beta \mid \beta \text{ is a root of } f(X)\}$.]

5.3 Algebraic closure

Lemma 5.17. Let F be a field. TFAE:

(i) F has no non-trivial algebraic extensions.

(ii) Irreducible polynomials in $F[X]$ have all degree 1.

(iii) Every polynomial in $F[X]$ splits in F.

Definition 5.18. A field satisfying the above equivalent conditions is called *algebraically closed*.

Theorem 5.19. $\mathbb{C}$ is algebraically closed.

[*Note:* We won't prove this.]

Lemma 5.20. Let K/F be a field extension. TFAE:

(i) K/F is algebraic and K is algebraically closed.

(ii) K/F is a maximal algebraic extension. (In other word, if M/K is a field extension and M/F is algebraic, then $M = K$).

(iii) K is algebraically closed and it is minimal among algebraically closed fields containing F. (In other words, if $F \subseteq M \subseteq K$ and M is algebraically closed, then $M = K$.)

(iv) K/F is algebraic and every polynomial in $F[X]$ splits in K.

[*Hint:* I find it easier to prove $(i) \implies (iv) \implies (ii) \implies (i) \iff (iii)$.]

Definition 5.21. If K/F satisfies the above equivalent conditions, then K is called an *algebraic closure* of F.

Lemma 5.22. Let K/F be a field extension. If K is algebraically closed, then K contains an algebraic closure of F.

Examples 5.23. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. What is an algebraic closure of $\mathbb{Q}$?

Theorem 5.24. Every field has an algebraic closure, and it is unique up to isomorphism.

[*Hint:* For existence use Zorn's lemma to build a maximal algebraic field extension. But beware! This appears to be a straightforward application of Zorn's Lemma, and yet there is a subtlety: if you miss it, you will fall victim to Russell's paradox. One way to avoid this subtlety is to notice that for a fixed field F, there is a cardinality $\mathcal{N}$ such that *every* algebraic field extension K/F has cardinality less than or equal to $\mathcal{N}$.

Alternatively, Proposition 30 on page 544 of the book offers a different proof.

For uniqueness, let F be a field and let K_1 and K_2 be two algebraic closures. Consider the set X of triples (M_1, M_2, φ) where $F \subseteq M_1 \subseteq K_1$ is an intermediate extension, $F \subseteq M_2 \subseteq K_2$ is an intermediate extension, and $\varphi : M_1 \to M_2$ is a field isomorphism such that $\varphi|_F = \mathrm{id}$. Define a partial order in X by saying that $(M_1, M_2, \varphi) \leq (N_1, N_2, \psi)$ iff $M_1 \subseteq N_1$, $M_2 \subseteq N_2$, and $\psi|_{M_1} = \varphi$. Use Zorn's lemma.]

6 Separable extensions

Definition 6.1. Let L be a field. A polynomial $f(X) \in L[X]$ is *separable* if it has no multiple roots in its splitting field; in other words, $f(X)$ is separable if $f(X)$ splits into *distinct* linear factors in its splitting field. (*Note:* Some authors give a different definition of separability for non-irreducible polynomials.)

Lemma 6.2. Let p be a prime. Let L be a field with characteristic p. Consider the map $\sigma_p : L \to L$ defined by $\sigma(a) = a^p$ for all $a \in L$. Then σ_p is a field homomorphism, called the *Frobenius homomorphism*. It is always injective. If L is finite, then σ_p is a bijection.

Examples 6.3.

(i) Give a few examples of irreducible separable polynomials. After you're done with this part, you should be feeling very skeptical that inseparable irreducible polynomials even exist.

(ii) Let p be a prime. Let $F = \mathbb{F}_p(T)$, where T is formal variable. Consider the polynomial $f(X) := X^p - T \in F[X]$. Prove that it is irreducible. Let K be a splitting field of $f(X)$ over F and let $\alpha \in K$ be a root of $f(X)$. Show that $f(X)$ splits in $K[X]$ in an unorthodox way. In particular, $f(X)$ is an irreducible, inseparable polynomial in $F[X]$. What is $\mathrm{Gal}(K/F)$? (*Note:* Make sure you understand the difference in "status" between X and T.)

Definition 6.4. Let K/F be an algebraic field extension. An element $\alpha \in K$ is called *separable over* F if $m_{\alpha,F}(X) \in F[X]$ is separable. The extension K/F is called *separable* if α is separable over F for every $\alpha \in K$.

Lemma 6.5. Let F be a field. Then TFAE:

(i) Every irreducible polynomial in $F[X]$ is separable.

(ii) Every algebraic extension K/F is separable.

Definition 6.6. If F satisfies the two equivalent conditions in the lemma above, then F is called *perfect*.

Definition 6.7. Let R be a ring. Suppose $f(X) = a_n X^n + \cdots + a_0 \in R[X]$. The *formal derivative of* $f(X)$ is the polynomial $Df(X) = na_n X^{n-1} + \cdots + 2a_2 X + a_1 \in R[X]$. Note that each coefficient is being "multiplied" by an integer using the action $\mathbb{Z} \times R \to R$.

Remark 6.8. $Df(x)$ is the same as the usual derivative $f'(x)$ from calculus, but in the context of algebra, you shouldn't think of the derivative as a "rate of change". (For that you need ϵ's and δ's – in other words, analysis.) Df is just a purely formal way of obtaining one polynomial from another[2]. Having said that,

[2]This is how most freshman calculus students think of derivatives anyway.

since Df *is* the same as f', we know that it obeys all the same rules: for all $f, g \in R[x]$, $n \in \mathbb{Z}$, and $a \in R$,

$$\begin{aligned} D(a) &= 0 \\ D(f+g) &= Df + Dg \\ D(fg) &= f \cdot Dg + g \cdot Df \\ D(af) &= aDf \\ D(f^n) &= nf^{n-1} \cdot Df \\ deg(Df) < deg(f) &\quad \text{or} \quad Df = 0 \end{aligned}$$

These are the rules on which we base all our calculations with Df.

Lemma 6.9. Let $R \subseteq S$ be PIDs with the same identity. Let $a, b \in R$ and let d be a greatest common divisor of a and b in R. Then d is also a greatest common divisor of a and b in S. In particular, we can talk about a and b being relatively prime without specifying where. (*Note:* This is not true for arbitrary domains.)

Proposition 6.10. Let F be a field. Let $f(X) \in F[X]$.

(i) Let α be a root of $f(X)$ in its splitting field. Then α is a multiple root of $f(X)$ iff α is also a root of Df.

(ii) $f(X)$ is separable iff $f(X)$ and $Df(X)$ are relatively prime.

(iii) If $f(X)$ is irreducible and inseparable, then $Df(X) = 0$.

Theorem 6.11. The only polynomials with zero derivative over a field with characteristic zero are the constants. Every field with characteristic zero is perfect.

Proposition 6.12. Let p be a prime and let F be a field with characteristic p. Let $f(X) \in F[X]$. Then $Df(X) = 0$ iff $f(X) = g(X^p)$ for some $g(X) \in F[X]$.

Theorem 6.13. Let p be a prime and let F be a field with characteristic p. Then F is perfect iff $F^p = F$.

Corollary 6.14. Every finite field is perfect.

Theorem 6.15.

(i) Let K/F be a finite field extension. Assume that $K = F(\alpha_1, \ldots, \alpha_n)$ and that α_j is separable over F for all j. Then K/F is separable.

(ii) The splitting field of a separable polynomial is separable.

(iii) The normal closure of a finite, separable field extension is a finite, normal, and separable field extension.

[*Note:* See homework #14.]

Exercise 6.16. Suppose that $K/M/F$ is a tower of field extensions. Show that if K/F separable, then both K/M and M/F are separable. (The converse is true too, but is more difficult to prove.)

7 The fundamental theorem of Galois theory

This corresponds to Sections 14.1 and 14.2 in the textbook. However, for this big theorem in particular, I am taking a completely different approach from the book, defining different concepts, and using and proving different lemmas. Hence, I am including a brief sketch of the proofs to help you. It should be enough for you to complete all the proofs, and the details will be provided in lecture as well. Notice that some of the result we need to prove as lemmas as part of this bigger proof are useful on their own!

7.1 The statement

Definition 7.1. A field extension K/F is a *Galois extension* when it is normal and separable.

Theorem 7.2. Let K/F be a finite Galois extension. Let $G = \mathrm{Gal}(K/F)$. Consider the maps $\widehat{I}$ and $\widehat{G}$ from Proposition 4.18.

(1) The maps $\widehat{I}$ and $\widehat{G}$ are inverses of each other. In other words:

- $\widehat{G}(\widehat{I}(H)) = \mathrm{Gal}(K/\operatorname{Inv}(H)) = H$ for every subgroup $H \leq G$.
- $\widehat{I}(\widehat{G}(M)) = \operatorname{Inv}(\mathrm{Gal}(K/M)) = M$ for every intermediate field $F \subseteq M \subseteq K$.

(2) Let $H \leq G$ and let $M = \widehat{I}(H)$, so that $H = \widehat{G}(M)$.
Then $|H| = [K : M]$. In particular $|G| = [K : F]$.
Equivalently, $|G : H| = [M : F]$.

(3) Under the same conditions as in Part 2, K/M is always Galois. In addition, TFAE:

- M/F is Galois.
- M/F is a normal field extension.
- H is a normal subgroup of G.

In that case, $\mathrm{Gal}(M/F) \cong \big(\mathrm{Gal}(K/F)\big) \,/\, \big(\mathrm{Gal}(K/M)\big)$.

Remark 7.3. Some general notes before we do this proof.

- For the rest of this section **we will assume that all field extensions are finite**.
- Review Propositions 4.6, 4.7, and 4.8.
- Review Theorems A and B.
- Recall that for an arbitrary field extension K/F and $H \leq \mathrm{Gal}(K/F)$ we only know that $H \leq \widehat{G}(\widehat{I}(H))$. Similarly, if M is an intermediate field, we only know that $M \subseteq \widehat{I}(\widehat{G}(M))$.
- A finite extension K/F is normal iff $m_{\alpha,F}(X)$ splits over K for all $\alpha \in K$. In other words, K/F is normal iff $m_{\alpha,F}(X)$ factors as product of degree-1 factors in $K[X]$ for all $\alpha \in K$. On the other hand K/F will be Galois iff $m_{\alpha,F}(X)$ factors as product of *distinct* degree-1 factors in $K[X]$ for all $\alpha \in K$.

Examples 7.4. Read all the examples on pages 559, 560, 563–566, 576–581 in the book.

7.2 Proof of Part 1

7.2.1 Proof of $\widehat{I}\widehat{G} = \mathrm{id}$

Lemma 7.5. Let K/F be a normal field extension. Let $f(X) \in F[X]$ be an irreducible polynomial. Then the action of the group $\mathrm{Gal}(K/F)$ on the set of roots of $f(X)$ in K is transitive. In other words, given $\alpha, \beta \in K$ which are both roots of $f(X)$ there is $\varphi \in \mathrm{Gal}(K/F)$ such that $\varphi(\alpha) = \beta$.

[*Hint:* Use Theorem A to extend $\mathrm{id} : F \to F$ to a field isomorphism $F(\alpha) \to F(\beta)$, and then Theorem B to extend it to a field isomorphism $K \to K$.]

Proposition 7.6. Let K/F be a Galois extension. Then $\mathrm{Inv}(\mathrm{Gal}(K/F)) = F$.

[*Hint:* Let $\alpha \in K \setminus F$. Prove that $m_{\alpha,F}(X)$ has a different root $\beta \in K$. Use Lemma 7.5 and conclude that $\alpha \notin \mathrm{Inv}(\mathrm{Gal}(K/F)$.]

Corollary 7.7. Let K/F be a Galois field extension. Then $\widehat{I}\widehat{G} = \mathrm{id}$.

[*Hint:* Given an intermediate field M, notice that K/M is Galois. Apply Proposition 7.6 to the extension K/M.]

Proposition 7.8. Let K/F be a field extension. Assume that $\mathrm{Inv}(\mathrm{Gal}(K/F)) = F$. Then K/F is Galois.

Note: We do not really need this result for the proof of the FTGT, but I am adding it here for completeness, since it is the reciprocal of 7.6

[*Hint:* Let $\alpha \in K$. Let $A = \{\sigma(\alpha) | \sigma \in \mathrm{Gal}(K/F)\}$. Let $q(X)$ be the polynomial whose roots are the distinct elements in A. Notice that $\mathrm{Gal}(K/F)$ acts in A. Prove that the coefficients of $q(X)$ lie in $\mathrm{Inv}(\mathrm{Gal}(K/F)) = F$. Conclude that $m_{\alpha,F}(X)$ splits in $K[X]$ and is separable.]

7.2.2 Proof of $\widehat{G}\widehat{I} = \mathrm{id}$

Definition 7.9. Recall that a field extension K/F is called *simple* if there is $\alpha \in K$ such that $K = F(\alpha)$. In that case, α is called a *primitive* element for K/F.

Proposition 7.10. Let K/F be a simple extension. Then $\widehat{G}\widehat{I} = \mathrm{id}$.

[*Hint:* Let $G = \mathrm{Gal}(K/F)$ and let $H \leq G$. Fix $\sigma \in \mathrm{Gal}(G/\mathrm{Inv}(H))$. We need to show that $\sigma \in H$. Assume that $K = F(\alpha)$. It is enough to show that $\sigma(\alpha) = \tau(\alpha)$ for some $\tau \in H$.

Let $A = \{\tau(\alpha) | \tau \in H\}$. Let $q(X)$ be the polynomial with roots the different elements in A. Prove that $q(X)$ has coefficients in $\mathrm{Inv}(H)$ so that $\sigma(\alpha)$ must be a root of $q(X)$.]

Lemma 7.11. Let K/F be a Galois field extension. Let $\alpha \in K$. TFAE:

- α is a primitive element for K/F.
- $\sigma(\alpha) \neq \alpha$ for all $\sigma \in \mathrm{Gal}(K/F) \setminus \{1\}$.

[*Hint:* One direction is easy. For the other, what is $\widehat{I}(\widehat{G}(F(\alpha)))$?]

Lemma 7.12. Let F be an infinite field. Let V be a finite dimensional vector space over F. Let $V_1, \ldots, V_n \subseteq V$ be subspaces. Assume $V_j \neq V$ for all j. Then $\bigcup_{j=1}^{n} V_j \neq V$.

[*Hint:* Use induction.]

Lemma. Let K/F be a normal field extension. Then $\mathrm{Gal}(K/F)$ is finite.

[*Hint:* K is the splitting field of some polynomial $f(X)$ over F. Consider the action of $\mathrm{Gal}(K/F)$ on the set of roots of $f(X)$ in K.]

Proposition 7.13. Every Galois extension is simple.

[*Hint:* If F is finite, use that $F^\times$ is cyclic.

Assume F is infinite. Let $G = \mathrm{Gal}(K/F)$. For each $\sigma \in G \setminus \{1\}$ define

$$V_\sigma := \{\alpha \in K \mid \sigma(\alpha) = \alpha\}$$

V_σ is proper subspace of K. Use Lemma 7.12 and the Lemma just above to find $\alpha \in K$ such that $\alpha \notin \bigcup_{\sigma \in G\setminus\{1\}} V_\sigma$. Then α is primitive for K/F by Lemma 7.11.]

Corollary 7.14. Part 1 of the Fundamental Theorem of Galois Theory (Theorem 7.2) is true.

[*Hint:* Use Corollary 7.7, Proposition 7.10, and Proposition 7.13.]

7.3 Proof of Part 2

Start with the hypothesis of the theorem. WMA $K = M(\alpha)$. Let $q(X)$ be the polynomial whose roots are the elements of $\{\sigma(\alpha) | \sigma \in H\}$. Prove that $q(X) = m_{\alpha,M}(X)$ and that $\deg q(X) = |H|$.

7.4 Proof of Part 3

Start with the hypothesis of the theorem.

- First assume M/F is normal. We want to show that $H \trianglelefteq G$. Prove that $\sigma(M) = M$ for all $\sigma \in G$. Let $\sigma \in G$, $\tau \in H$, $a \in M$. Notice that it is enough to show that $\sigma\tau\sigma^{-1}(a) = a$. Prove it.
- Now assume that $H \trianglelefteq G$. We want to show that M/F is normal.

  Let $\alpha \in M$ and let $f(X) = m_{\alpha,F}(X)$. We want to show that $f(X)$ splits in M. We know $f(X)$ splits in K. Let $\beta \in K$ be a root of $f(X)$. We want to show that $\beta \in M$.

  Let $\tau \in H$. It is enough to show that $\tau(\beta) = \beta$. Use Lemma 7.5 to construct $\varphi \in G$ such that $\varphi(\alpha) = \beta$. Notice that $\varphi^{-1}\tau\varphi(\alpha) = \alpha$ and conclude from there.
- As K/F is separable, so is M/F.
- Finally, assume that M/F is a normal extension and that $H \trianglelefteq G$. Consider the map

$$\begin{array}{rccc} T: & \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(M/F) \\ & \sigma : K \to K & \mapsto & \sigma|_M : M \to M \end{array}$$

Prove it is well-defined, it is a group homomorphism, and it is surjective (use Theorem B). Prove that $\ker T = H$ and apply the First Isomorphism Theorem.

8 Cyclotomic extensions and constructibility of polygons

Remark 8.1. First recall what we already know. We defined Δ_2 to be the set of complex numbers which can be constructed with straightedge and compass starting from the numbers $\{0, 1\}$. We said that a field extension K/F is *2-filtered* if there is a sequence of subextensions $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ such that $[K_j : K_{j-1}] = 2$ for all j. Then, given $z \in \mathbb{C}$, we proved that TFAE:

(i) $z \in \Delta_2$

(ii) There is a 2-filtered field extension $K/\mathbb{Q}$ such that $z \in K$.

In particular, if $[\mathbb{Q}(z) : \mathbb{Q}]$ is not a power of 2, then $z \notin \Delta_2$. We also showed that a regular n-gon is constructible with straightedge and compass iff $\zeta_n := e^{2\pi i/n} \in \Delta_2$. Finally, review Problem 1 from Homework #13.

Definition 8.2. For any field L and any positive integer n we define $\mu_n(L)$ to be the set of roots of the polynomial $X^n - 1$ in L. If there is no ambiguity, we will write μ_n instead of $\mu_n(L)$.

Lemma 8.3. Let L be a field and n a positive integer.

(i) μ_n is a group with respect to multiplication.

(ii) μ_n is a cyclic group.

(iii) Assume $X^n - 1$ splits over L and that the characteristic of L does not divide n. Then $|\mu_n| = n$.

(iv) If $d|n$ then $\mu_d \subseteq \mu_n$.

Proposition 8.4. Let F be a field and let K be the splitting field of $X^n - 1$ over F. Let $\mu_n := \mu_n(K)$. Then $K = F(\mu_n)$. Consider the map

$$\begin{array}{rccc} T: & \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Aut}\,\mu_n \\ & \sigma : K \to K & \mapsto & \sigma|_{\mu_n} : \mu_n \to \mu_n \end{array}$$

where $\mathrm{Aut}\,\mu_n$ means the automorphism group of the group μ_n. Then T is a well-defined, injective group homomorphism. In particular, $\mathrm{Gal}(K/F)$ is abelian.

Definition 8.5. Let L be a field and let $z \in L$. We say that z is an *n–th root of unity* if z is a root of $X^n - 1$. We say that z is a *primitive n-th root of unity* if it is an n-th root of unity but it is not a d-th root of unity for any $d < n$. Notice that this agrees with Definition 3.16 when $L = \mathbb{C}$.

Lemma 8.6. Let L be a field. Assume that $X^n - 1$ splits over L and that the characteristic of L does not divide n.

(i) Let $z \in \mu_n$. Then z is a primitive n-th root of unity iff $\mu_n = \langle z \rangle$.

(ii) Let z be a primitive n-th root of unity. Then $\mu_n = \{1, z, z^2, \ldots, z^{n-1}\}$. Moreover, z^m is another primitive n-th root of unity iff $(m, n) = 1$.

(iii) Let $z \in \mu_n$. Then there exists a unique $d|n$ such that z is a primitive d-th root of unity.

Definition 8.7. For the rest of this section, let K_n be the splitting field of $X^n - 1$ over $\mathbb{Q}$ and let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Notice that $K_n = \mathbb{Q}(\zeta_n)$. We refer to $K_n/\mathbb{Q}$ as the *n-th cyclotomic extension.* Define

$$\Phi_n(X) := \prod_{\substack{0<m<n \\ (n,m)=1}} (X - \zeta_n^m) = \prod_{\substack{z \text{ is a primitive} \\ n\text{-th root of unity in } \mathbb{C}}} (X - z)$$

We refer to $\Phi_n(X)$ as the *n-th cyclotomic polynomial.* Notice that, for the moment $\Phi_n(X) \in K_n(X)$.

Proposition 8.8.

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Lemma 8.9. The coefficients of $\Phi_n(X)$ lie in $\mathbb{Z}$.

[*Hint:* First, show that the coefficients of $\Phi_n(X)$ are invariant under $\mathrm{Gal}(K_n/\mathbb{Q})$, and hence $\Phi_n(X) \in \mathbb{Q}[X]$. Second, use induction and Gauss lemma to show that $\Phi_n(X) \in \mathbb{Z}[X]$.]

Theorem 8.10. The polynomial $\Phi_n(X)$ is monic and irreducible in $\mathbb{Z}[X]$, and hence irreducible in $\mathbb{Q}[X]$.

[*Note:* It is enough to prove that if ω is a root of $\Phi_n(X)$ and p is a prime that does not divide n, then ω and ω^p have the same minimal polynomial. For the details, see Theorem 41 on page 554 of the book.]

Corollary 8.11. The minimal polynomial of ζ_n over $\mathbb{Q}$ is $\Phi_n(X)$. In particular

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n),$$

where φ is the Euler function.

Corollary 8.12.

(i) For every n, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In particular if p is a prime, then $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq Z_{p-1}$.

(ii) Let p be prime. Then a regular p-gon is constructible with straightedge and compass iff p is a Fermat prime (i.e. $p - 1$ is a power of 2).

(iii) Let p be an odd prime and let $m \geq 2$. Then a regular p^m-gon is not constructible with straightedge and compass.

Theorem 8.13. Let n be an integer and let φ be the Euler function. Then TFAE:

(i) A regular n-gon is constructible with straightedge and compass.

(ii) $n = 2^c p_1 \cdots p_r$ where $c \geq 0$ and $p_1, \ldots, p_r$ are different Fermat primes.

(iii) $\varphi(n)$ is a power of 2.

Exercise 8.14. Find an explicit expression for $\cos \frac{2\pi}{5}$ and for $\cos \frac{2\pi}{17}$ in terms of rational numbers, the field operations, and square roots.

[*Hint:* This process is outlined on page 602 of the book.]

9 Finite fields

Remark 9.1. First, recall what we already know. Let K be a finite field. Then we know its characteristic is a prime p. Moreover, the field with p elements $\mathbb{F}_p$ is the prime subfield of K, so that $\mathbb{F}_p \subseteq K$. Hence K is a (finite dimensional) vector space over $\mathbb{F}_p$ so that $|K| = p^n$ for some integer n.

We had defined the Frobenius homomorphism $\sigma_p : K \to K$ by $\sigma_p(a) = a^p$ for all $a \in K$. Notice that $\sigma_p \in \mathrm{Gal}(K/\mathbb{F}_p)$.

Proposition 9.2. Let p be a prime and $n > 1$.

(i) Let K be the splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. Then $|K| = p^n$.

(ii) Let K be a field of size p^n. Then K is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$.

[*Hint:* For the first part, let Σ be the set of roots of $X^{p^n} - X$ in K. Notice that Σ is a field so $\Sigma = K$. Notice that $X^{p^n} - X$ is separable.

For the second part, recall that the group $K^\times$ is cyclic.]

Definition 9.3. The above proposition shows that there exists a unique field of order p^n up to isomorphism. We will denote it by $\mathbb{F}_{p^n}$.

Lemma 9.4. The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple.

[*Hint:* The group $\mathbb{F}_{p^n}^\times$ is cyclic.]

Corollary 9.5. For every prime p and every positive integer n there exist an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n.

Proposition 9.6. The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. The Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism σ_p.

Proposition 9.7. For every divisor $d|n$ there is one intermediate subfield of $\mathbb{F}_{p^n}/\mathbb{F}_p$ isomorphic to $\mathbb{F}_{p^d}$. Those are all the intermediate subfields.

Example 9.8. Let $F = \mathbb{F}_2$. Let $K = F[X]/(X^4 + X^3 + X^2 + X + 1)$. Describe $\mathrm{Gal}(K/F)$ and draw the lattice of subextensions of K/F. For each subfield $F \subseteq M \subseteq K$ find $\alpha \in M$ such that $M = F(\alpha)$ and find the irreducible polynomial of α over K.

Theorem 9.9. The polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ factors as the product of all the irreducible, monic, polynomials of degree d in $\mathbb{F}_p[X]$, where d runs through the positive divisors of n, with none of the irreducibles repeated.

[*Hint:* Let $f(X) := X^{p^n} - X \in \mathbb{F}_p[X]$. Prove that $f[X]$ is separable. Prove that every irreducible factor of $f(X)$ has degree a divisor of n. Next, let $g(X) \in \mathbb{F}_p[X]$ be an irreducible polynomial with degree $d|n$. Prove that $g(X)$ has a root in a field isomorphic to $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, where it splits, and hence all roots of $g(X)$ are roots of $f(X)$.]

Corollary 9.10. Let $\lambda_p(n)$ be the number of irreducible, monic polynomials in $\mathbb{F}_p[X]$ of degree n. Then

$$p^n = \sum_{d|n} d\lambda_p(d).$$

Example 9.11. Find all irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$.

Exercise 9.12. How many irreducible polynomials of degree 9 are there in $\mathbb{F}_5[X]$?

Proposition 9.13. Let p be a prime. If $m|n$ we can say that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Hence we can define $K = \bigcup_{m=1}^{\infty} \mathbb{F}_{p^m}$. (This requires some interpretation.) Then K is an algebraic closure of $\mathbb{F}_p$.

10 Solvability of polynomial equations by radicals

This corresponds to Sections 14.6 and 14.7 in the textbook. However, the book does things differently and in much greater generality. Hence, like in Section 7, I am including a brief sketch of the proofs to help you. It should be enough for you to complete all the proofs, and the details will be provided in lecture as well.

Throughout this section, all fields will be assume to be of characteristic zero. Hence every field extension is separable. We will also assume every field extension to be finite and every group to be finite.

10.1 Radical extensions

Definition 10.1. A field extension K/F is called *radical* if there are fields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ and elements $\alpha_j \in K_j$ for $j = 1, \ldots, m$ such that

- $K_j = K_{j-1}(\alpha_j)$, and
- $\alpha_j^{n_j} \in K_{j-1}$ for some positive integer n_j.

If we let $\beta_j := \alpha_j^{n_j} \in K_{j-1}$ we can then write $K_j = K_{j-1}(\sqrt[n_j]{\beta_j})$. The elements $\alpha_1, \ldots, \alpha_m$ are called a *radical sequence* for K/F.

Notice that we may assume that all n_j are prime if we need so.

Example 10.2. Find a radical sequence for $K/\mathbb{Q}$, where $K = \mathbb{Q}\left(\sqrt[4]{\dfrac{3+\sqrt[3]{2+\sqrt{5}}}{1-\sqrt{5}}}\right)$.

Remark 10.3. Beware of a common point of confusion. It is not the same thing to say that "K/F is generated by an element of degree n" and "K/F is generated by an n-th root". Write down what these two statements mean formally and notice the difference. Notice that Proposition 3.8 says that the two statements *are* equivalent when $n = 2$.

Definition 10.4. A polynomial $f(x) \in F[X]$ is called *solvable by radicals (over F)* if there are fields $F \subseteq K \subseteq E$ such that

- K is the splitting field of $f(X)$ over F, and
- E/F is radical.

This means that all the roots of $f(X)$ can be written in terms of F, the field operations, and arbitrary roots. Notice that we do not request that K/F is radical, but only that it is contained in a radical extension. The following example shows that these two conditions are not the same.

Example 10.5. Let $E := \mathbb{Q}(\zeta_7)$. Clearly $E/\mathbb{Q}$ is radical. We also know it is a normal extension with Galois group Z_6. In particular, every subextension is normal.

Let $M = \mathbb{Q}(\alpha)$ where $\alpha = \zeta_7 + \zeta_7^6 = 2\cos\frac{2\pi}{7}$. Notice that $\mathbb{Q} \subseteq M \subseteq E$, that $M = E \cap \mathbb{R}$, and that $[M : \mathbb{Q}] = 3$. Show that $M/\mathbb{Q}$ is not radical.

This means that we can express $\alpha \in \mathbb{R}$ in terms of radicals, but not in terms of real radicals! More explicitly:

$$\cos\frac{2\pi}{7} = \frac{\sqrt[3]{7}}{6}\left[\sqrt[3]{\frac{1+3\sqrt{-3}}{2}} + \sqrt[3]{\frac{1-3\sqrt{-3}}{2}} - 1\right]$$

(For a more precise discussion that we can't express α using only real radicals, see pages 633–634 in the book.)

Definition 10.6. The Galois group of the polynomial $f(X) \in F[X]$ is $\mathrm{Gal}(K/F)$, where K is the splitting field of $f(X)$ over F. We will denote if by $\mathrm{Gal}(f(X), F)$.

Remark 10.7. Our goal is to prove that a polynomial is solvable by radicals if and only if its Galois group is solvable.

10.2 Review: solvable groups

Definition 10.8. Let $\mathcal{P}$ be a property that groups may have. Let G be a group. A *$\mathcal{P}$-tower* for G is a finite sequence of groups $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$ such that H_j/H_{j-1} is $\mathcal{P}$ for all j. (Notice that we do not request H_j to be normal in G.)

Example 10.9. We proved that every finite group has a simple-tower. We called it a composition series. Moreover, in such a tower the quotients H_j/H_{j-1} depend uniquely on G (up to reordering and isomorphism), and we called them the invariant factors of G.

Remark 10.10. Using the 3rd/4th isomorphism theorem, if $H \trianglelefteq G$ we can put together a $\mathcal{P}$-tower for H and a $\mathcal{P}$-tower for G/H to get a $\mathcal{P}$-tower for G.

Definition 10.11. A group is called *solvable* if it has an abelian tower.

Proposition 10.12.

(i) Let G be a group and let $H \leq G$. If G is solvable, then H is solvable.

(ii) Let G be a group and let $H \trianglelefteq G$. Then G is solvable iff H and G/H are solvable.

Corollary 10.13. Let $F \subseteq M \subseteq K$ be fields. Assume that K/F and M/F are normal. Then $\mathrm{Gal}(K/F)$ is solvable iff $\mathrm{Gal}(K/M)$ and $\mathrm{Gal}(M/F)$ are solvable.

Lemma 10.14. Let G be a group. TFAE:

(i) G is solvable.

(ii) G has a cyclic-tower.

(iii) G has a (cyclic of order prime)-tower.

(iv) G has a solvable-tower.

Example 10.15. Every abelian group is solvable, and so are D_{2n} and S_4. A_5 is not solvable. A_n and S_n, with $n \geq 5$, are not solvable.

10.3 If a polynomial is solvable by radicals, then its Galois group is solvable

Proposition 10.16. Let F be a field where the polynomial $X^n - 1$ splits. Let K/F be a field extension such that $K = F(\alpha)$ for a certain $\alpha \in K$ such that $a := \alpha^n \in F$. Then K is the splitting field of $X^n - a$ over F and $\mathrm{Gal}(K/F)$ is cyclic.

[*Hint:* Consider the map $\sigma \in \mathrm{Gal}(K/F) \to \sigma(\alpha)/\alpha \in \mu_n$. Prove that it is a well-defined, injective group homomorphism.]

Remark 10.17. Consider Propositions 8.4 and 10.16 together. Think of how they suggest that the Galois group of a radical extension is solvable.

Proposition 10.18. Let K/F be a normal, radical extension. Then $\mathrm{Gal}(K/F)$ is solvable.

[*Hint:* Let us write $K = F(\alpha_1, \ldots, \alpha_m)$ such that $\alpha_j^{n_j} \in F(\alpha_1, \ldots, \alpha_{j-1})$ for some positive integers n_j. We will do induction on the length m of the radical sequence $\alpha_1, \ldots, \alpha_m$.

Let E_1 be the splitting field of $X^{n_1} - 1$ over K and let $E_0 \subseteq E_1$ be a splitting field of $X^{n_1} - 1$ over F. Notice that $E_1 = E_0(\alpha_1, \ldots, \alpha_m)$. Let $M = E_0(\alpha_1)$. By induction hypothesis, $\mathrm{Gal}(E_1/M)$ is solvable. Using Proposition 10.16, $\mathrm{Gal}(M/E_0)$ is solvable. Using Proposition 8.4, $\mathrm{Gal}(E_0/F)$ is solvable. Use Proposition 10.12 repeatedly (checking that what needs to be normal is normal) to conclude that $\mathrm{Gal}(K/F)$ is solvable.]

Lemma 10.19. The composite of two radical extension is a radical extension. In particular, if K/F is a radical extension, then its normal closure is also a radical extension.

[*Hint:* Use Proposition 5.16.]

Theorem 10.20. Let $f(X) \in F[X]$ be a polynomial which is solvable by radicals over F. Then $\mathrm{Gal}(f(X), F)$ is solvable.

[*Hint:* Let K be the splitting field of $f(X)$ over F. Assume that $K \subseteq R$ such that R/F is radical. Let E/F be the normal closure of R/F. Use Lemma 10.19 and Proposition 10.12 to conclude that $\mathrm{Gal}(K/F)$ is solvable.]

10.4 An example of a polynomial which is not solvable by radicals

Consider the polynomial $f(X) = X^5 - 6X + 3 \in \mathbb{Q}[X]$. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$.

Show that $f(X)$ is irreducible using Gauss lemma and Eisenstein criterion. Hence, it has five different roots and $G \leq S_5$.

Use calculus to prove that $f(X)$ has exactly three real roots, and two non-real roots which are complex conjugate of each other. Notice that complex conjugation is an element of G. Hence G contains a transposition (as a subgroup of S_5).

Let $\alpha \in K$ be a root of $f(X)$. Let $M = \mathbb{Q}(\alpha)$ and let $H = \mathrm{Inv}(M)$. Notice that $|G : H| = 5$, hence $|G|$ is a multiple of 5. Now G contains an element of order 5, which must be a 5-cycle (as a subgroup of S_5).

Show that S_5 is the only subgroup of S_5 which contains a transposition and a 5-cycle.

Conclude that $\mathrm{Gal}(f(X), \mathbb{Q})$ is S_5, and hence not solvable, so that $f(X)$ is not solvable by radicals over $\mathbb{Q}$. Not only there isn't a universal formula to solve polynomials of degree 5 like there is a quadratic formula for polynomials of degree 2, but the roots of this specific polynomial cannot be written in terms of radicals at all!

10.5 The reciprocal of Section 10.3

Lemma 10.21. Let K/F be a field extension. Let $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(K/F)$ be *different* elements in the Galois group. Assume there are $t_1, \ldots, t_m \in F$ such that $t_1\sigma_1 + \cdots + t_m\sigma_m = 0$ (as a function $K \to K$). Then $t_1 = \cdots = t_m = 0$.

[*"Hint":* This is Theorem 7 on page 569 on the book.]

Proposition 10.22. Let K/F be a normal field extension and let $G = \mathrm{Gal}(K/F)$. Assume that G is cyclic of order n. Assume that $X^n - 1$ splits in F. Then there exists $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^n \in F$. (In particular, the extension K/F is radical.)

[*Hint:* Let $\beta \in K$, $\theta \in \mu_n$, and $\sigma \in G$. We define the Lagrange Resolvent by

$$R_{\beta,\theta,\sigma} := \beta + \theta\sigma(\beta) + \theta^2\sigma^2(\beta) + \cdots + \theta^{n-1}\sigma^{n-1}(\beta) \in K.$$

Prove that $\sigma^k(R_{\beta,\theta,\sigma}) = \theta^{-k}(R_{\beta,\theta,\sigma})$ for all k.

Let us choose σ to be a generator of G. Conclude that $(R_{\beta,\theta,\sigma})^n$ is invariant under G, and hence in F.

Choose also θ to be a primitive n-th root of unity. Let $\alpha := R_{\beta,\theta,\sigma}$, where we have chosen β so that $\alpha \neq 0$ (this is possible by Lemma 10.21). Show that α is not fixed by any non-identity element of G and conclude that α satisfies the conditions in the statement of the proposition.]

Theorem 10.23. Let K/F be a normal extension and let $G = \mathrm{Gal}(K/F)$. Let $n = |G|$. Assume that G is solvable and that $X^n - 1$ splits in F. Then K/F is radical.

[*Hint:* We do induction on n. Pick a normal subgroup $H \trianglelefteq G$ such that G/H is cyclic of order m for some $m > 1$, $m|n$. The corresponding subextension M/F is radical by Proposition 10.22. K/M is radical by induction hypothesis. Hence K/F is radical.]

Theorem 10.24. Let K/F be a normal field extension. Assume that $\mathrm{Gal}(K/F)$ is solvable. Then there exists a field extension R/K such that R/F is radical.

[*Hint:* Let $G = \mathrm{Gal}(K/F)$ and let $n = |G|$. Let K_1 be the splitting field of $X^n - 1$ over K. Let $F_1 \subseteq K_1$ be the splitting field of $X^n - 1$ over F. Notice that K_1/F_1 is normal, as K/F is normal.

Define a map

$$\begin{array}{rccc} T: & \mathrm{Gal}(K_1/F_1) & \longrightarrow & \mathrm{Gal}(K/F) \\ & \sigma : K_1 \to K_1 & \mapsto & \sigma|_K : K \to K \end{array}$$

Prove that T is a well-defined, injective group homomorphism. Hence $\mathrm{Gal}(K_1/F_1)$ is solvable. Use Theorem 10.23 to conclude that K_1/F_1 is radical. Notice that F_1/F is radical. Take $R = K_1$.

Corollary 10.25. Let $f(X) \in F[X]$. Then $f(X)$ is solvable by radicals over F if and only if $\mathrm{Gal}(f(X), F)$ is a solvable group.

[*Hint:* Put Theorems 10.20 and 10.24 together.]