Intro to Galois Theory

Vihaan Dheer

1 Field Extensions

1.1 Finite and Algebraic Extensions

See Notes, MATH 250B / Crash Course / Intro.

Here's an observation we will use implicitly all the time.

Lemma 1.1.1 *Let L/K be any extension, and suppose $f, g \in K[x]$ are such that $f \mid g$ over $L[x]$. Then $f \mid g$ over $K[x]$.*

Proof Let $h \in L[x]$ such that $fh = g$. Choose $q, r \in K[x]$ such that $\deg r < \deg f$ and $g = qf + r$. Then $r = (g - q)f$, so for degree reasons $r = 0$ and $g = q \in K[x]$. □

Lemma 1.1.2 *Let R be a UFD, $L = \mathrm{Frac}(R)$, and $f, g \in L[x]$ are monic polynomials such that $fg \in R[x]$. Then $f, g \in R[x]$.*

Proof Since fg is monic with coefficients in R, then its content is 1, so $\mathrm{cong}(f)\mathrm{cont}(g) = 1$ by Gauss' lemma. Since each one is monic, the content is in between 0 and 1, so both must have content 1 and thus they lie in $R[x]$. □

Our application will be either $R = \mathbb{Z}$ or $R = K[t]$ for a field K, so that $L = \mathbb{Q}$ or $K(t)$.

1.2 Splitting Fields and Algebraic Closure

Definition 1.2.1 Let K be a field. A splitting field for $f \in K[x]$ is an extension L/K such that:

1. f splits into linear factors over L.
2. If $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ over L, then $L = K(\alpha_1, \ldots, \alpha_n)$.

Proposition 1.2.2 *Let $f \in K[x]$. Then f has a splitting field.*

Proof Let $K_0 = K$ and write $f = p_1 p_2 \cdots$ where $p_i \in K[x]$ is irreducible. Then let $K_1 = K_0[x]/(p_1)$, assuming $\deg p_1 > 1$. If the image of f splits into linear factors in K_1, then we stop, if not repeat with $K_2, K_3, \ldots$. And this process has to stop because there are only finitely many factors and finitely many degrees. Then, at the end, f splits into linear factors, and it is generated by the roots of f because at each stage we have only added the roots of f. □

Proposition 1.2.3 *Let $p \in K[x]$, and suppose L, L' be two splitting fields. Then $L/K \cong L'/K$.*

Proof Suppose instead $K \cong K'$, p corresponds to p', and we have splitting fields of p and p'. Factor $p = p_1 p_2 \cdots$, and then extend $K \subset K(\alpha_1)$, and we can extend the isomorphism to $K(\alpha_1) \to L$ by mapping α_1 to some root we selected, and we can inductively extend to a map of $L \to L'$. Hence $[L : K] \leq [L' : K']$, then reversing the argument shows that L and K have the same degrees. Hence our map constructed must be an isomorphic. □

Definition 1.2.4

1. A field K is *algebraically closed* if every polynomial $f \in K[x]$ splits into linear factors over K.
2. An *algebraic closure* of a field K is an algebraic extension L of K which is algebraically closed.

Proposition 1.2.5 *Any field has an algebraic closure.*

Proof By the axiom of choice, well-order the polynomials in $K[x]$ as $\{f_\alpha : \alpha\}$. We construct the algebraic closure by transfinite recursion, so that each K_α will be an algebraic extension of K_0: set $K_0 = K$, if K_α has been constructed we let $K_{\alpha+1}$ be a splitting field of $f_\alpha \in K[x] \subset K_\alpha$, which is a finite hence algebraic extension. If α is a limit ordinal, we let $K_\alpha = \bigcup_{\beta<\alpha} K_\beta$, which is an algebraic extension (clear). Now let $\bar{K} \coloneqq \bigcup_\alpha K_\alpha$, where the ordinals are just going up until $\aleph_0 \cdot |K|$.

Now $\bar{K}/K$ is an algebraic extension, and clearly all polynomials of K have a root in $\bar{K}$ because we have adjoined them. But, if $p(x) \in \bar{K}[x]$, let $p(x) = \alpha_n x^n + \cdots \alpha_0$, then $p(x)$ is a polynomial in the finite extension

$$K(\alpha_0, \ldots, \alpha_n)/K,$$

to which we can adjoin a root β (which is not necessarily in $\bar{K}$), then $K(\alpha_0, \ldots, \alpha_n, \beta)$ is a finite extension of K, so let $m(x) \in K[x]$ be the minimal polynomial of β. Then m has a root γ in $\bar{K}$, so $p(\gamma) = 0$. □

If $S \subset K[x]$ is a set of polynomials, we say a splitting field of S is an extension L/K over which every polynomial $f \in S$ splits over L, and L is generated over K by the roots of all polynomials in S.

We claim that L/K is an algebraic closure if and only if it is a splitting field of $K[x]$. ($\Rightarrow$) is clear because all polynomials in $L[x]$ (and so $K[x]$) split into linear factors over L, and in addition L/K is algebraic, so every element $\alpha \in L$ is a root of a polynomial in $K[x]$. On the other hand, if L/K is a splitting field of all of $K[x]$, first note it is algebraic; any $\alpha \in L$ can be written

$$\alpha = a_n\beta^n + \cdots + a_1\beta_1 + a_0,$$

where $a_i \in K$ and the β_i are roots of polynomials in $K[x]$. In particular, we have a finite chain

$$K \subset K(\beta_1) \subset K(\beta_1, \beta_2) \subset \cdots \subset K(\beta_1, \cdots, \beta_n)$$

of finite extensions, so the over all extension is finite so algebraic, and it contains α. Thus L is algebraic over K. To show L is algebraically closed, it suffices to show that every monic irreducible polynomial in $L[x]$ has a root in L (so in particular is linear). If

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \in L[x]$$

is such a polynomial, then it is also monic irreducible over the finite extension

$$K_1 = K(\alpha_0, \ldots, \alpha_{n-1})/K,$$

so we may adjoin a root β (in some other extension), and the extension $K_1(\beta)$ is again finite so β has a minimal polynomial $p_\alpha \in K[x]$. Since f is itself the minimal polynomial of β in $K_1[x]$, $f \mid p_\beta$ in $K_1[x]$ and hence in $L[x]$. But p_β splits into linear factors over L, so since f is irreducible it must be equal (up to unit) to one of these linear factors.

If L/K is an algebraic extension, then elements $\alpha, \beta \in L$ are *conjugate (over K)* if they have the same minimal polynomial. Then clearly this is equivalent to one satisfying the minimal polynomial of the other, and if $\alpha, \beta \in K$, then they are conjugate iff $\alpha = \beta$. Also note in this case that there's a canonical isomorphism $K(\alpha) \xrightarrow{\sim} K(\beta)$ over K sending $\alpha \mapsto \beta$, as both are canonically isomorphic to $K[x]/(m(x))$ where m is the common minimal polynomial. The following result, alongside the earlier discussion, will show uniqueness of algebraic closure.

Theorem 1.2.6 *Let K be a field and $S \subset K[x]$. Then any two splitting fields of S are isomorphic over K.*

Lemma 1.2.7 *Let L/K be an algebraic extension and let $\sigma\colon L \to L$ be a map over K. Then σ is an automorphism.*

Proof First, if $p \in K[x]$, observe that $p(\sigma(\alpha)) = \sigma(p(\alpha))$, so in particular σ takes roots of p to roots of p, and hence permutes the set of roots of p.

We have to show σ is surjective; let $\alpha \in L$ and let $p_\alpha \in K[x]$ be its minimal polynomial, and let $\alpha = \alpha_0, \ldots, \alpha_n$ be the roots of p_α in L, then

$$K_1 = K(\alpha_0, \ldots, \alpha_n)/K$$

is a finite extension and now know $\sigma(K_1) \subset K_1$ because σ sends roots to roots. Since K_1 is finite dimensional over K and σ is an injective linear map, $\sigma(K_1) = K_1$, thus $\alpha \in \sigma(L)$. □

If L/K is any extension, we write $\mathrm{Gal}(L/K)$ for the *Galois group* of automorphisms over K. The lemma shows that if L/K is algebraic, the set of homomorphisms over K is equal to the Galois group.

Proof (of Thm. 1.2.6) Let L, L' be two splitting fields of S, and enumerate the polynomials in S by $\{f_i : i \in I\}$ by ordinals; we construct by transfinite recursion for each i an extension $K \subset L_i \subset L$ equipped with a map $\mu_i \colon L_i \to L'$ over K, such that $i \leq j$ implies $L_i \subset L_j$ and $\bigcup_i L_i = L$.

Let $L_0 = K$, and in general if L_i has been constructed let $L_{i+1} = L_i(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the distinct roots of f_i in L_i. Then choose a root $\beta_1 \in L$ of the image of the minimal polynomial of α_i under μ_i. Then since $L_i(\alpha_1) = L_i[x]/(p_{\alpha_1})$, we can extend μ_i to a map $L_i(\alpha_1) \to L'$ by sending $\alpha_1 \mapsto \beta_1$. Now, let $p_{\alpha_2} \in L_i(\alpha_1)[x]$ be the minimal polynomial of α_2 over $L_i(\alpha_1)$, then we can look at the image of p_{α_2} under the extended map in L', and since $p_{\alpha_2} \mid f_i$, the image divides f_i as well, so L' contains a root of it, β_2 (since it has all roots of f_i). Hence we can extend to $L_i(\alpha_1, \alpha_2) \to L'$, and so on, until we have extended to $\mu_{i+1} \colon L_{i+1} \to L'$.

If j is a limit ordinal, then we set $L_j = \bigcup_{i<j} L_i$, and then μ_j is already determined by extending μ_i for each $i < j$. Finally, pick $\alpha \in L$, and since L is generated over K by the roots of all the $\{f_i\}$, there are finitely many $\alpha_1, \ldots, \alpha_n$ such that

$$\alpha \in K(\alpha_1, \ldots, \alpha_n)$$

and α_k is a root of f_{i_k}. Taking $\bar{i} = \max_k i_k$, all the f_j until f_i split over $L_{\bar{i}}$, so $\alpha \in L_{\bar{i}}$. It follows that $L = \bigcup_i L_i$, and hence our maps μ_i extend to $L \to L'$ over K.

To complete the proof, since L and L' were arbitrary there are ring maps $\mu_1 \colon L \to L'$ and $\mu_2 \colon L' \to L$ both over K. Therefore $\mu_1\mu_2 \colon L' \to L'$ is a map over K, so it is an automorphism by Lemma 1.2.7. In particular, $L' = \mu_1(\mu_2(L')) \subset \mu_1(L)$, so $\mu_1 \colon L \to L'$ is onto. □

Corollary 1.2.8 *Let K be a field.*

1. *K has an algebraic closure $\overline{K}$ which is unique up to isomorphism over K.*
2. *Any set $S \subset K[x]$ of polynomials has a splitting field L/K, which is unique up to isomorphism over K.*

Proof We have previously shown the existence in (1) and the theorem gives the uniqueness in (2). Taking $S = K[x]$, that gives the uniqueness in (1). For existence in (2), take the algebraic closure $\overline{K}$ and let $L \subset \overline{K}$ be the K-subalgebra containing K generated by all roots of all polynomials in S in $\overline{K}$. A priori it is just an intermediate ring, but in fact it is a field: For $\alpha \in L$, we know $K \subset K[\alpha] \subset L$, but since α is algebraic $K[\alpha] = K(\alpha)$, so in fact $\alpha^{-1} \in L$, which is what we wanted. □

Example 1.2.9 Any nontrivial algebraic extension of $\mathbb{R}$ (e.g. any finite extension) is of degree 2. Indeed, if $L/\mathbb{R}$ is algebraic then let $\overline{\mathbb{R}}$ be an algebraic closure containing L (i.e. take an algebraic closure of L), then since $\overline{R} \cong \mathbb{C}$ over $\mathbb{R}$, $[L : \mathbb{R}] = 2 = [\overline{R} : L][L : \mathbb{R}]$, so $[L : \mathbb{R}] \leq 2$. It follows that any irreducible polynomial with coefficients in $\mathbb{R}$ is quadratic or linear, because the extension $\mathbb{R}[\alpha]$ has degree at most 2.

Remark 1.2.10 We can easily extend this result to the case of isomorphic fields: Namely, if $\mu\colon K \cong K'$ and $S \subset K[x]$, and L is a splitting field of S while L' is a splitting field of $\mu(S)$, then μ extends to an isomorphism $L \cong L'$. To see this, let $L'' \supset K$ be the extension in which we use μ to replace elements of $\mu(K')$ with those of K. Then $L'' \cong L'$ is μ on the subfield K, and the identity on the rest of L''. Then L'' is a splitting field of S, so $L \cong L''$ over K, and hence $L \cong L'$ over μ.

Corollary 1.2.11 *Let L/K be a splitting field of a set S of polynomials and let $\alpha, \beta \in L$ be two conjugate elements over K. Then there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.*

Proof Since $\alpha, \beta \in L$, it follows that L is also a splitting field for S as a set of polynomials over $K(\alpha)$ and over $K(\beta)$. Considering the canonical isomorphism $K(\alpha) \xrightarrow{\sim} K(\beta)$, the above remark gives an automorphism $L \to L$ extending $K(\alpha) \to K(\beta)$, which is over K. □

Corollary 1.2.12 *Let $\sigma\colon K \to F$ be a map of fields with F algebraically closed. Then σ extends to $\overline{K}$, any algebraic closure of K. If $F/\sigma(K)$ is algebraic, then the extension is an isomorphism.*

Proof This follows easily from Remark 1.2.10. Namely, let $\overline{\sigma(K)}$ be the algebraic closure of $\sigma(K)$ inside F; then the isomorphism $K \xrightarrow{\sim} \sigma(K)$ lifts to an isomorphism $\overline{K} \xrightarrow{\sim} \overline{\sigma(K)}$ of splitting fields, so composing with the inclusion gives the result. If F was algebraic over $\sigma(K)$, then $\overline{\sigma(K)} = F$. □

1.3 Finite Fields and Separable Extensions

Let us recap some facts we already know. Let $\phi\colon K \to L$ be a map of fields, and let α be an algebraic element over K (in some extension). How can we extend ϕ to $\phi'\colon K(\alpha) \to L$? Well, we know $K(\alpha) \cong K[x]/(p_\alpha)$ given by $\alpha \mapsto x$

is an isomorphism, so the extensions of ϕ to $K(\alpha)$ are in bijection with the roots of $p_\alpha^\sigma \in L[x]$, where p_α is the minimal polynomial.

In particular, take ϕ to be the inclusion $K \hookrightarrow \overline{K}$, and let $\alpha \in \overline{K}$ be some element algebraic over K of degree n (that is, $\deg(p_\alpha) = [K(\alpha) : K] = n$). Then the number of possible extensions is just given by the number of distinct roots of the minimal polynomial of α in $\overline{K}$. This number represents the notion of *separability*.

Definition 1.3.1 Let L/K be a field extension.

1. A polynomial $f \in K[x]$ is *separable* if there is an algebraic closure $\overline{K} \supset K$ such that f has no repeated roots.
2. An algebraic element $\alpha \in L$ over K is separable if its minimal polynomial is separable over K. An algebraic extension L/K is separable if every element of L is separable over K.

Recall that if $f \in K[x]$ is a polynomial, its *derivative* $f' \in K[x]$ is a polynomial defined by

$$(a_n x^n + \cdots + a_1 x + a_0)' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1.$$

Proposition 1.3.2 *Let $f \in K[x]$ be a polynomial of degree n. The following are equivalent:*

(i) f is separable over K.

(ii) There exists an extension L/K in which f has n distinct roots.

(iii) $(f, f') = 1$ in $K[x]$, that is f is coprime to its derivative.

(iv) In any extension where f splits into linear factors, it splits into distinct linear factors.

Proof $(i) \Rightarrow (ii)$ is by definition, so let L/K be an extension as in (ii). There are $\alpha_1, \ldots, \alpha_n \in L$ and $a \in K^\times$ such that

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n).$$

So, if f' has a non-unit common factor with f then there must be some i such that $(x - \alpha_i) \mid f'$. On the other hand, we can write

$$f'(x) = \sum_{k=1}^{n} \prod_{j \neq k} (x - \alpha_j) \Rightarrow f'(x) - \sum_{k \neq i} \prod_{j \neq k} (x - \alpha_j) = \prod_{k \neq i} (x - \alpha_k).$$

So $(x - \alpha_i)$ divides the LHS, and thus much divide the RHS, so $\alpha_i = \alpha_j$ for some j, a contradiction, proving (iii). Now assuming $(f, f') = 1$, let L be an extension over which f splits, and suppose some factor is repeated so that $f(x) = (x - \alpha)^2 g(x)$ for some g. Then $f' = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$, so

$(x - \alpha)$ divides both f and f', a contradiction. Finally, $(iv) \Rightarrow (i)$ is obvious because $\overline{K}$ is such an extension. □

Observe that an element $\alpha \in L$ over K if and only if it is a root of a separable polynomial in $K[x]$, because given such an f, we must have $p_\alpha \mid f$ so any repeated roots in of p_α in $\overline{K}$ would give repeated roots of f. We can apply this notion to the question we started with: If α is a separable element over K, then the number of extensions of $K \hookrightarrow \overline{K}$ to $K(\alpha)$ is exactly the degree of α over K.

Proposition 1.3.3 *Let K be a field of characteristic zero. Then every irreducible polynomial $f \in K[x]$ is separable. In particular, all algebraic extensions in characteristic zero are separable.*

Proof In characteristic zero, any degree > 2 polynomial has degree > 1, so if it is irreducible then it cannot have any nonzero factors. □

This shows why it is hard for a polynomial, and thus an element, to be inseparable. We would need its minimal polynomial to have derivative zero, which can only happen under the specific circumstance that the polynomial is made up of monomials that are powers of x divisible by the characteristic.

Example 1.3.4 Let us compute $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. $\mathbb{C} = \mathbb{R}[i]$ and the minimal polynomial is $x^2 + 1$ which has two distinct roots over $\mathbb{C}$, i and $-i$. Any extension of $\mathbb{R} \hookrightarrow \mathbb{C}$ to $\mathbb{C}$ hence is determined (and given) by sending i to i or $-i$, so $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \bar{\cdot}\}$. If $f(x) \in \mathbb{R}[x]$, this means that for any root α, $\bar{\alpha}$ is a root. Hence the non-real roots come in pairs, i.e. there are always an even number of them. In particular, every polynomial of odd degree has a real root, and more generally it has an odd number of real roots.

We may axiomize the properties discussed above.

Definition 1.3.5 A field K is *perfect* if every irreducible polynomial $f \in K[x]$ is separable.

Proposition 1.3.6 *Let K be a field. The following are equivalent:*

(i) K is perfect.

(ii) Any irreducible polynomial $f \in K[x]$ has nonzero derivative.

(iii) Every finite (or algebraic) extension of K is separable.

(iv) Either K has characteristic 0, or if $\mathrm{char}(K) = p > 0$, then every element of K is a pth power.

(v) Either K has characteristic 0, or if $\mathrm{char}(K) = p > 0$, then the Frobenius $x \mapsto x^p$ is an automorphism.

Proof We already know that $(i) \Leftrightarrow (ii)$. $(i) \Rightarrow (iii)$ is trivial, and conversely suppose every finite extension is separable. Letting f be an irreducible polynomial, applying a previous proposition to a splitting field of f shows that f has distinct roots and so is separable.

Moving on, (iv) and (v) are obviously equivalent; let us suppose one of the first three and prove (iv). If K is characteristic p, let $a \in K$ and consider $f(x) = x^p - a$. Let L/K be a splitting field of f and choose a root $\beta \in L$ with minimal polynomial p_β over K that is separable. But the Frobenius map $(-)^p \colon L \to L$ is at least injective, so if β' is another root than $(\beta')^p = a = \beta^p$ implies $\beta' = \beta$. Since f splits over L, it follows that

$$f(x) = (x - \beta)^p \in L[x],$$

but now p_β is a monic polynomial which has β as a root, divides f, and has distinct roots. Therefore $p_\beta = x - \beta \in K[x]$, so $\beta \in K[x]$ is our pth root.

Lastly, assume $(iv)/(v)$, then it suffices to do the case of $\mathrm{char}(K) = p > 0$ by the previous proposition. Let $f \in K[x]$ be a polynomial with zero derivative. If $f(x) = a_n x^n + \cdots + a_0$, it follows that $i a_i = 0$ for all i, so either $a_i = 0$ or $p \mid i$. Therefore we can rewrite

$$f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \cdots b_1 x^p + b_0.$$

By our assumption, let $g(x) = b_m^{1/p} x^m + \cdots b_1^{1/p} x + b_0^{1/p}$, then by Frobenius we have $f(x) = g(x)^p$. As $p \geq 2$, f cannot be irreducible which proves that in this case (ii) holds. □

As a brief aside, we mention a more difficult result which has practical applications in algebraic geometry.

Proposition 1.3.7 *Let L/K be a separable extension and A be a reduced K-algebra. Then $A \otimes_K L$ is reduced.*

Proof See [STK, Lemma 030U] for details, but the general steps are as follows:

1. If $A \otimes_K L$ is not reduced, then there are finitely generated K-subalgebras $A' \subset A$ and $L' \subset L$ such that $A' \otimes_K L'$ is not reduced ([STK, Lemma 00I3]). So we may assume A is of finite type over k and L is finitely generated over K.
2. Since A is of the form $K[x_1, \ldots, x_n]/I$, it is a reduced Noetherian ring and has finitely many minimal primes $\mathfrak{p}_1, \ldots \mathfrak{p}_r$. Therefore its total ring of fractions is given by

$$A \hookrightarrow Q(A) = Q(A/\mathfrak{p}_1) \times \cdots Q(A/\mathfrak{p}_r),$$

that is A embeds into a finite product of fields. If $A \otimes_K L$ is not reduced, then $(A/\mathfrak{p}_i) \otimes_K L$ is not reduced for some i. So we may assume A is a domain.

The rest of the result now follows from [STK, Lemma 030U]. □

Corollary 1.3.8 *Let k be a perfect field and X a reduced scheme over k. Then the base change $X \times_k \operatorname{Spec}(\overline{k})$ is reduced over $\overline{k}$.*

Let us return to Galois theory. In the remainder of this section we will compute all finite fields and study their properties. Let K be a finite field. It cannot have characteristic zero since in that case it would contain a copy of $\mathbb{Q}$, so suppose the characteristic is $p > 0$. Then there is an embedding $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z} \to K$, so K is a vector space over $\mathbb{F}_p$, and must be of the form $K \cong \bigoplus_{i \in I} \mathbb{F}_p$ as a vector space. Then I must have finite cardinality n, so $|K| = |\mathbb{F}_p|^n = p^n$ for some n.

Now we show the existence of a field of order p^n for any p and n. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, and let $L/\mathbb{F}_p$ be a splitting field of this polynomial. Clearly $f'(x) = -1$, so f has p^n distinct roots in L, call them $R = \{\alpha_1, \ldots, \alpha_{p^n}\}$. By inspection $0, 1 \in R$, and

$$f(\alpha_i \alpha_j) = \alpha_i^{p^n} \alpha_j^{p^n} - \alpha_i \alpha_j = \alpha_i \alpha_j - \alpha_i \alpha_j = 0.$$

The sum of two roots is again a root because of the Frobenius map, and if α is a root then $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. Therefore R is a field. Notice that if $x \in \mathbb{F}_p$, then since $\left|\mathbb{F}_p^\times\right| = p - 1$, $x^p = x$, so $x^{p^n} = x$. Hence $\mathbb{F}_p \subset R \subset L$, and R is a field extension with p^n elements. In particular, $[R : \mathbb{F}_p] = n$, and $R = \mathbb{F}_p[\alpha_1, \ldots, \alpha_{p^n}]$, and so in fact $R = L$ is a splitting field for $f(x)$. It follows that each $\alpha_i \in R$ satisfies a polynomial of degree $\leq n$. Since f is separable and each $\alpha \in R$ is a root of it, R is a separable extension.

By construction, each element of R is its own p^nth root. Therefore, any $\alpha \in R$ can be written $(\alpha^{p^{n-1}})^p$, so every element of R is a pth power and thus R is a perfect field (but, we already knew this because $\mathbb{F}_p$ is perfect and R is an algebraic extension of it, so any algebraic extension of R is one of $\mathbb{F}_p$ and therefore is separable). We will denote this constructed field $\mathbb{F}_{p^n}$.

Theorem 1.3.9 (structure of finite fields) *Let K be a finite field. Then $\operatorname{char} K = p > 0$, and there is a unique n such that $K \cong \mathbb{F}_{p^n}$ over the embedding $\mathbb{F}_p \to K$, which has p^n elements. $\mathbb{F}_{p^n}$ is a perfect field and a degree n separable extension of $\mathbb{F}_p$, and is characterized up to isomorphism over $\mathbb{F}_p$ as a splitting field of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Proof We have already shown most of this, all that remains is uniqueness. Let $F \subset K$ be the canonical subfield isomorphic to $\mathbb{F}_p$, then we know K is a finite extension of degree $[K : F] = n$, so it has p^n elements for some $n > 0$. Then $K^\times$ is a group of order $p^n - 1$, so for all $\alpha \in K^\times$, $\alpha^{p^n - 1} = 1$, i.e. $\alpha^{p^n} - \alpha = 0$, that is all elements of K satisfy $f(x) = x^{p^n} - x \in F[x]$. It can't have more than p^n distinct roots, so

$$x^{p^n} - x = \prod_{\alpha \in K} (x - \alpha) \qquad \text{in } K[x],$$

so K is a splitting field of x^{p^n}, and hence is isomorphic to $\mathbb{F}_{p^n}$. □

Hence we found every finite field. We now make some observations about how to work with them in practice. Given any monic irreducible polynomial f of degree n over $\mathbb{F}_p$, we observe that adjoining a root (i.e. taking $\mathbb{F}_p[x]/(f)$), $\mathbb{F}_p(\alpha)$, gives a degree n extension of $\mathbb{F}_p$, which therefore must be $\mathbb{F}_{p^n}$. In particular, by adjoining the root α, we get all roots of $x^{p^n} - x$. Let us see that we can do this for all p and n.

Lemma 1.3.10 *Any finite subgroup of the multiplicative group of a field is cyclic. In particular, every finite field has cyclic multiplicative group.*

Proof Let F be a finite field of order q, then $F^\times$ has order $q-1$ and is a finite abelian group. If it is not cyclic, then its cyclic decomposition into primes is not square free, so there is some $p_0 \mid q-1$, such that $(\mathbb{Z}/p_0\mathbb{Z})^2 \subset F^\times$ is a direct summand of F. Hence there are at least p_0^2 elements of $\mathbb{F}^\times$ which satisfy the equation $x^p - 1$, but this polynomial can have at most p_0 roots in F. □

If L/K is an extension, we say an algebraic element $\alpha \in L$ is a *primitive element* if $L = K(\alpha)$.

Corollary 1.3.11 *Any extension of finite fields has a primitive element.*

Proof Let $\mathbb{F}_{q_1}/\mathbb{F}_{q_0}$ be the extension, which is finite so algebraic. The lemma shows that $(\mathbb{F}_{q_1})^\times$ has a multiplicative generator α, so $\mathbb{F}_{q_0}(\alpha)$ must be the whole field $\mathbb{F}_{q_1}$. □

Incidentally, this also gives a fun proof that for each prime $p > 0$ and any n, there is an irreducible polynomial mod p in degree n: take the minimal polynomial of the primitive element of $\mathbb{F}_{p^n}/\mathbb{F}_p$. Therefore, we can always write $\mathbb{F}_{p^n}$ as given by adjoining a root of any polynomial degree n irreducible polynomial over $\mathbb{F}_p$. Let us study the Galois group of this extension. Write $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ with (degree n) minimal polynomial $f_\alpha \in \mathbb{F}_p[x]$. We know that any extension σ of the inclusion $\mathbb{F}_p \to \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ is the same as the choice of a root of f_α which exists in $\mathbb{F}_{p^n}$ (to send α to). By Lemma 1.2.7, these are exactly the automorphisms over $\mathbb{F}_p$, and moreover since α is a root of $x^{p^n} - x$, we know $f_\alpha \mid x^{p^n}$, so there are n distinct roots of f_α all contained in $\mathbb{F}_p(\alpha)$. So far, this already implies that $G \coloneqq \mathrm{Gal}(\mathbb{F}_{p^n})/\mathbb{F}_p)$ has n elements, each given by sending α to a root of f_α. We will later show that $G = \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.3.12 (primitive element theorem) *Let L/K be an extension finitely generated by separable elements. Then L/K has a primitive element. In particular, every finite separable extension has a primitive element.*

Proof We already showed this if K is finite. Therefore assume K is an infinite field, and by induction on the number of generators, we may further assume $L = K(\beta, \gamma)$. Let us work in some algebraic closure $\overline{K} \supset K(\beta, \gamma) \supset K$.

Let $a \in K$ be an element such that $\alpha = \beta + a\gamma \in K(\beta, \gamma)$ is not primitive, i.e. $K(\alpha) \subsetneq K(\beta, \gamma)$. Let f, g be the minimal polynomials of β and γ resp. *over* $K(\alpha)$. Taking F to be the splitting field of $\{f, g\}$ inside $\overline{K}$, this must also contain $K(\alpha, \beta)$.

Since $\gamma \notin K(\alpha)$, $\deg g > 1$ and since γ is separable over K (and thus $K(\alpha)$), γ has a conjugate $\gamma \neq \gamma' \in F$ over $K(\alpha)$. By Cor. 1.2.11, there is a $\sigma \in \mathrm{Gal}(F/K(\alpha))$ mapping $\gamma \mapsto \gamma'$ and fixing α. This means

$$\beta + a\gamma = \alpha = \sigma(\alpha) = \sigma(\beta) + a\gamma',$$

so $a = (\beta - \sigma(\beta))/(\gamma' - \gamma)$. Finally, if $\{\alpha_i\}$ and $\{\beta\}$ are all conjugates of α and β in $\overline{K}$ over the base K, then we have shown (at least) that

$$\beta + a\gamma \text{ not primitive } \implies a \in \left\{ \frac{\beta - \beta_i}{\gamma_j - \gamma} : i, j, \gamma_j \neq \gamma \right\}.$$

Thus, we will have found a primitive element if we can choose any $a \in K$ not contained in the set on the RHS; but indeed, that set is finite and K, so we can always choose this. □

It is in fact true that an extension is generated by separable elements if and only if it is separable, but we will delay the proof slightly. Furthermore, in the previous proof we cannot yet say that the primitive element we constructed is separable itself. All of these shortcomings will be magically fixed by proving basic results about Galois theory, so they should serve as a motivator. For the time being, there is one nice corollary that we can prove.

Corollary 1.3.13 *Let L/K be a (possibly infinite) separable extension, and suppose there exists n such that $\deg \alpha \leq n$ for all $\alpha \in L$. Then L/K is finite and $[L : K] \leq n$.*

Proof The boundedness means that there is some $\alpha \in L$ with maximal degree, and we claim $K(\alpha) = L$. Indeed, if $\beta \in L$, then $K(\alpha, \beta)$ is finitely generated by separable elements so has a primitive element $\gamma \in L$ with $K(\gamma) = K(\alpha, \beta)$. This means

$$\deg \gamma = [K(\alpha, \beta) : K(\alpha)] \deg \alpha,$$

but the maximality means $\deg \gamma \leq \deg \alpha$, and thus $[K(\alpha, \beta) : K(\alpha)] = 1$, i.e. $\beta \in K(\alpha)$. Hence $[L : K] = [K(\alpha) : K] = \deg \alpha \leq n$. □

1.4 Normal and Galois Extensions

Let us begin with a motivating lemma:

Lemma 1.4.1 *Let L/K be a finite extension contained in an algebraic closure $\overline{K}$. Then the number of extensions of the inclusion $K \hookrightarrow \overline{K}$ to L is at most $[L : K]$. If in addition L/K is finitely generated by separable elements, then this is an equality.*

Proof Write $L = K(\alpha_1, \ldots, \alpha_n)$, and if we are in the second case then assume the α_i are separable. We prove both cases simultaneously by induction on n, and in the base case where $L = K$ obviously the only extension of $K \to \overline{K}$ to K is just $K \to \overline{K}$. Assuming the result has been proven for $n-1$, let p_{α_n} be the minimal polynomial of α_n over $K_{n-1} \coloneqq K(\alpha_1, \ldots, \alpha_{n-1})$, which has at most $[L : K_{n-1}]$ distinct roots in $\overline{K}$. An extension of any map $K_{n-1} \to \overline{K}$ to L is determined by sending α_n to one of its distinct roots in $\overline{K}$, so there are less than $[L : K_{n-1}]$ of those. Since there are at most $[K_{n-1} : K]$ extensions to K_{n-1} by induction, there are at most $[L : K]$ extensions to L.

If instead we are in the second case, then at the nth step there are exactly $[L : K_{n-1}]$ extensions because α_n is separable over K and therefore over K_{n-1} as well. Note also that it is impossible for two extensions to have been distinct at the $(n-1)$th stage and then become the same at the nth stage (because we are extending maps), so this completes the proof. □

Corollary 1.4.2 *For a finite extension L/K, we have $|\mathrm{Gal}(L/K)| \leq [L : K]$.*

Proof Taking an algebraic closure $\overline{K} \supset L$, each distinct automorphism $L \to L$ over K gives a distinct extension of $K \hookrightarrow L \hookrightarrow \overline{K}$ to L (by just post-composing with the inclusion $L \hookrightarrow \overline{K}$), so we're done by the lemma. □

The lemma shows that it can often be fruitful to think about field extensions L/K in terms of the set of maps $L \to \overline{K}$ extending the inclusion $K \hookrightarrow \overline{K}$. This will be crucial for Galois theory.

Proposition 1.4.3 *Let L/K be an algebraic extension. The following are equivalent:*

(i) Any irreducible polynomial $f \in K[x]$ which has a root in L, splits into linear factors over L.

(ii) L is a splitting field of a set of polynomials in $K[x]$.

(iii) If $\overline{K} \supset L \supset K$ is an algebraic closure, then any map $L \to \overline{K}$ over K factors through $L \hookrightarrow \overline{K}$.

(iv) If $\overline{K} \supset L \supset K$ is an algebraic closure, then any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ preserves L. In particular $\sigma|_L \in \mathrm{Gal}(L/K)$.

Definition 1.4.4 If an algebraic extension L/K satisfies any of these equivalent conditions, L/K is called a *normal extension*.

Proof (of Prop. 1.4.3) $(i) \Rightarrow (ii)$: Let $S \subset K[x]$ be the set of minimal polynomials of all elements of L. Since all the elements in L are roots of these, L is generated by the roots of polynomials in S. On the other hand, each such polynomial is irreducible and has a root in L, so it splits over L by assumption.

$(ii) \Rightarrow (iii)$: Let S be the set of polynomials and $\sigma\colon L \to \overline{K}$ be such a map over K; since L is generated by the roots of polynomials in S, it suffices to

show that for any $f \in S$ and $\alpha \in L$ such that $f(\alpha) = 0$, $\sigma(\alpha) \in L$. Considering $K \subset K(\alpha) \subset L$, σ must map α to a root of the minimal polynomial $p_\alpha \in K[x]$; since $p_\alpha \mid f$, such a root is also a root of f, and hence it must be contained in L as f splits over L. Therefore $\sigma(\alpha) \in L$.

(iii) $\Rightarrow$ *(iv)*: This is obvious because $\sigma|_L \colon L \to \overline{K}$ is as above, so it must map into L. That $\sigma|_L \colon L \to L$ is an automorphism follows from Lemma 1.2.7.

(iv) $\Rightarrow$ *(i)* Let f be irreducible with root $\alpha \in L$, take an algebraic closure $\overline{K} \supset L$, and suppose $\beta \in \overline{K}$ is another root of f. Then $\alpha, \beta \in \overline{K}$ have the same minimal polynomial over K, i.e. they are conjugate. So, applying Cor. 1.2.11 to the set of polynomials $K[x]$, there is an automorphism $\overline{K} \to \overline{K}$ mapping $\alpha \mapsto \beta$. Any such map by assumption preserves L, so $\beta \in L$. □

It happens frequently that finite extensions we consider are not normal. For example, consider $x^3 - 2 \in \mathbb{Q}[x]$. It has only one real root, namely $\sqrt[3]{2}$, so the other two roots are complex. Hence it is an irreducible polynomial which has a root in $\mathbb{Q}(\sqrt[3]{2})$, but doesn't split in that (degree 3) extension. Instead, we must add one of the other roots which is of degree 2 over $\mathbb{Q}(\sqrt[3]{2}$, so the overall splitting field will have degree 6. A positive example is the finite fields we constructed in the last section. This is obvious because $\mathbb{F}_{p^n}/\mathbb{F}_p$ was the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Let L/K be an extension with Galois group $G = \mathrm{Gal}(L/K)$. For any subgroup $H \subset G$, we define the *fixed field of* H to be the subset

$$L^H \coloneqq \{\alpha \in L : \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}.$$

By definition $K \subset L^H \subset L$, and in fact L^H is a field. Since each $\sigma \in H$ is a ring homomorphism, it is clear that L^H is closed under addition and multiplication, and if $\alpha \in L^H$ then

$$\sigma(\alpha^{-1})\alpha = \sigma(\alpha^{-1}\alpha) = 1 \Rightarrow \sigma(\alpha^{-1}) = \alpha^{-1}.$$

It is obvious e.g. that $L^{\{1\}} = L$. Dually, suppose that $K \subset L \subset F$ are extensions, and let $G = \mathrm{Gal}(F/K)$. Then each automorphism $\sigma \in \mathrm{Gal}(F/L)$ is also an automorphism over K, so we view this as a subgroup

$$\mathrm{Gal}(F/L) \leq \mathrm{Gal}(F/K) \quad \leftrightarrow \quad K \subset L \subset F.$$

By definition, each element $\sigma \in \mathrm{Gal}(F/L)$ (as a subgroup) fixes L, therefore $L \subset F^{\mathrm{Gal}(F/L)}$. A question which Galois theory will help answer is whether L is *exactly* the intermediate extension which is fixed by $\mathrm{Gal}(F/L)$.

Theorem 1.4.5 *Let L/K be a finite extension with Galois group $G = \mathrm{Gal}(L/K)$. Then following conditions are equivalent:*

(i) L/K is separable and normal.

(ii) L/K is normal and finitely generated by separable elements.

(iii) $[L : K] = |G|$.

(iv) $L^G = K$.

(v) L *is a splitting field of a separable polynomial in* $K[x]$.

Definition 1.4.6 A finite extension L/K satisfying any of these equivalent conditions is called a *Galois* extension.

Proof We first show that (i) through (iv) are equivalent. $(i) \Rightarrow (ii)$ is trivial by taking any finite generating set. For $(ii) \Rightarrow (iii)$, by Lemma 1.4.1 and choosing $\overline{K} \supset L$, we know that the number of extensions of $K \hookrightarrow \overline{K}$ to $L \to \overline{K}$ is exactly $[L : K]$. But since L is normal over K, every $L \to \overline{K}$ factors through $L \hookrightarrow \overline{K}$ and gives an element of the Galois group, so the inclusion induces a bijection

$$G = \mathrm{Gal}(L/K) \cong \mathrm{Hom}_K(L, \overline{K}).$$

We have just said the RHS has has $[L : K]$ elements completing the proof.

For $(iii) \Rightarrow (iv)$, always $L \subset L^G$ holds. Note that $\mathrm{Gal}(L/L^G) \leq G$ as usual, but G also fixes L^G so $G \subset \mathrm{Gal}(L/L^G)$, and therefore the two groups are equal, so there are exactly $[L : K]$ automorphisms $L \to L$ fixing L^G by assumption. Notice that each such automorphism gives a distinct extension of the inclusion $L^G \hookrightarrow \overline{K}$ to L, so there are at least $[L : K]$ extensions, and by Lemma 1.4.1 there are at most $[L : L^G]$ such extensions. Therefore

$$[L : K] \leq \left|\{\text{ext. of } L^G \hookrightarrow \overline{K}\}\right| \leq [L : L^G] \leq [L : K],$$

thus $[L : L^G] = [L : K]$ so $L^G = K$.

We will now show $(iv) \Rightarrow (i), (v)$, which proves that the first four are equivalent and imply (v). As above, remember

$$|G| \leq \left|\{\text{ext. of } L \hookrightarrow \overline{K}\}\right| \leq [L : K],$$

so at least G is finite. Fix $\alpha \in L$ and consider the finite set $\{\sigma(\alpha) : \sigma \in G\}$, where we label its (distinct) elements $\{\alpha, \beta_1, \ldots, \beta_n\}$ since $\mathrm{Id} \in G$. Write

$$p(x) = (x - \alpha)(x - \beta_1) \cdots (x - \beta_n) \in L[x],$$

and suppose its expansion is $p(x) = \sum_i b_i x^i \in L[x]$. For any $\sigma \in G$, σ just bijectively permutes the roots $\alpha, \beta_1, \ldots, \beta_n$, and $(x - \alpha)^\sigma = x - \sigma(\alpha)$, so $p^\sigma(x) = p(x)$. Then

$$\sum_i \sigma(b_i) x^i = p^\sigma(x) = p(x) = \sum_i b_i x^i,$$

so $\sigma(b_i) = b_i$ for all i. Since σ was arbitrary, $b_i \in L^G = K$, so $p(x) \in K[x]$ and thus α is a root of a separable polynomial over K. Since α was arbitrary this shows L/K is separable.

In the same fashion, now choose $\alpha_1, \ldots, \alpha_n \in L$ generating L over K, and again write $\{\beta_j\} = \{\sigma(\alpha_i) : i, \sigma \in G\}$. Then G acts on (permutes) the β_i, and so the resulting polynomial

$$p(x) = (x - \beta_1) \cdots (x - \beta_m)$$

once again has $p^\sigma = p$, so it follows that $p(x) \in K[x]$. But now since $\mathrm{Id} \in G$, each α_i is one of the β_j, so α_i is a root of $p(x)$, and thus L is generated by the roots of $p(x)$. But by construction p is also a separable polynomial which splits over L, so L is a splitting field for p proving (v). By Prop. 1.4.3 this implies L/K is normal, proving (i) as well.

Finally, that remains is to show (v) implies one of the first four, so we do $(v) \Rightarrow (ii)$. Letting p be the polynomial, again by Prop. 1.4.3 the extension is normal. But now p factors into its distinct roots in L, and by definition of a splitting field they generate L. Each of those generators are a root of the separable polynomial p, so they are separable. □

We will remember the fact from the proof used multiple times that $|\mathrm{Gal}(L/K)| \leq [L : K]$ for any finite extension L/K. Also, observe that if $\{f_1, \ldots, f_n\}$ is a finite set of separable polynomials, then a splitting field for it will be normal and finitely generated by separable elements, so in (v) we may take finitely many polynomials. Even though we have not yet gotten to the fundamental theorem of Galois theory, we did some nontrivial work in this proof. For example, we can (finally) prove the following proposition.

Corollary 1.4.7 *Let L/K be an algebraic extension.*

1. *L/K is separable if and only if L is generated over K by separable elements.*
2. *The set $L_{\mathrm{sep}} \subset L$ of separable elements of L over K is a separable extension $K \subset L_{\mathrm{sep}} \subset L$, which we call the separable closure of K in L.*

Proof For (1), one direction is obvious so suppose L/K is generated by a set of separable elements $\{\alpha_i : i \in I\}$, then each $\beta \in L$ is a polynomial in some finite subcollection, so write $\beta \in K(\alpha_{i_1}, \ldots, \alpha_{i_n})$. Take a splitting field F containing this extension of the set $\{p_{\alpha_{i_j}} : j = 1, \ldots n\}$ of (separable) minimal polynomials in $K[x]$, then

$$\beta \in K(\alpha_{i_1}, \ldots, \alpha_{i_n}) \subset F,$$

but F/K is a Galois extension and hence is separable, so β is separable.

For (2), let $\alpha, \beta \in L_{\mathrm{sep}}$, then by (1) $K(\alpha, \beta)$ is a separable extension so $K(\alpha, \beta) \supset L_{\mathrm{sep}}$. It is clear then $K \subset L_{\mathrm{sep}}$, $\alpha^{-1}, \alpha\beta, \alpha + \beta \in L_{\mathrm{sep}}$. Finally, L_{sep} is obviously separable since it consists of separable elements. □

We have now multiple times used the following technique: we are given an algebraic extension L/K (e.g. $L = K(\alpha_1, \ldots, \alpha_n)$) and we want to take the

splitting field of the minimal polynomials of α_i to get a normal extension containing L. We can do this in two ways: first, view the minimal polynomials as polynomials in $L[x]$, then take their splitting field to an extension of L, and finally observe that it is also a splitting field of those polynomials over K. Alternatively, we can take an algebraic closure of K containing L (i.e. one of L), and then take the subfield generated by all conjugates of elements of L.

We call this construction a *normal closure* of L over K; indeed, any normal extension of K containing L must contain splitting fields for these minimal polynomials. The normal closure is, like a splitting field, unique up to choice of algebraic closure. Note that if L/K is a finite separable extension, then a normal closure is clearly Galois.

Motivated by Thm. 1.4.5, if L/K is a (not necessarily finite) algebraic extension, then we will call it Galois if it is separable and normal. Let K be a field and $\overline{K}$ an algebraic closure. The *(absolute) separable closure* L of K is the separable closure of K in $\overline{K}$. This is a maximal Galois extension: Indeed, it contains every separable extension, and on the other hand if an irreducible polynomial f has a root α in L, $K(\alpha)$ is a finite separable extension so its normal closure (inside $\overline{K}$) is a finite Galois extension so is contained in L. In particular, f splits over L.

Lemma 1.4.8 *Let L/K be a finite Galois extension with $\alpha_1 \in L$, and write $X = \{\alpha_1, \dots \alpha_n\}$ for the set of conjugates of α.*

1. *The Galois group acts transitively on X.*
2. *If α is a primitive element, then it acts simply transitively on X.*

Proof This is almost immediate from Thm. 1.4.5. For the first statement, apply Cor. 1.2.11, and for the second observe that $|X| = n = |G|$, so if it acts transitively it must act freely too. □

As an example, let us compute the Galois group of the finite extension $\mathbb{F}_q/\mathbb{F}_p$ where $q = p^n$. We defined it to be a splitting field of $x^{p^n} - x$, which is separable, so the extension is Galois. Since its degree is n, the Galois group G has order n. Consider the Frobenius map

$$\sigma \colon \mathbb{F}_q \to \mathbb{F}_q \qquad x \mapsto x^p.$$

If $a \in \mathbb{F}_p$, then $a^{p-1} = 1$ so σ fixes $\mathbb{F}_p$ and hence $\sigma \in G$. We claim that σ has order n, i.e. $G \cong \mathbb{Z}/n\mathbb{Z}$ generated by σ. Indeed, suppose $k < n$ and $\sigma^k = 1$. Recalling that $\mathbb{F}_q^\times$ is cyclic of order $q-1$, let α be a generator; then

$$\alpha = \sigma^k(\alpha) = \sigma^{k-1}(\alpha^p) = \sigma^{k-2}(\alpha^{p^2}) = \cdots = \alpha^{p^k}.$$

This means that $\alpha^{p^k - 1} = 1$, so $p^k = 1$, thus $k = 0$; so we have shown:

Proposition 1.4.9 *Let $q = p^n$. The extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois with Galois group $\mathbb{Z}/n\mathbb{Z}$ generated by the Frobenius automorphism $x \mapsto x^p$.*

Note that in the above proof we were careful to *not* write $\sigma^k(\alpha) = (\sigma(\alpha))^k$, which is of course not true. In the next section, we will finally prove the 'fundamental theorem of Galois theory', which will actually let us compute things. Before doing so, let us generalize the argument we gave at the end of proving Thm. 1.4.5.

Theorem 1.4.10 (Artin's theorem) *Let L be an extension and $G \leq \mathrm{Aut}(L)$ a finite group of automorphisms. Then L/L^G is a finite Galois extension with Galois group G.*

Proof First we prove L/L^G is separable; if $\alpha_1 \in L$, let $\{\alpha_1, \ldots, \alpha_n\}$ be the set of *distinct* conjugates of α_1 under G, i.e. the set $\{\sigma(\alpha_1) : \sigma \in G\}$. This is a G-set because $\sigma\alpha_i = \sigma(\sigma'(\alpha_1)) = (\sigma\sigma')\alpha_1 = \alpha_k$ for some k. Let f be the separable polynomial

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in L[x],$$

then each σ just permutes the roots so $f^\sigma = \sigma$, and thus $f \in L^G[x]$. Therefore α_1 is the root of a separable polynomial in $L^G[x]$, and since it was arbitrary, L/L^G is separable.

If p_α is the minimal polynomial of $\alpha = \alpha_1$, then $p_\alpha \mid f$, so in particular, $\deg \alpha \leq n \leq |G|$. It follows from Cor. 1.3.13 that the extension is finite and $[L : L^G] \leq |G|$. Moreover $p_\alpha \mid f$ means that p_α splits over L. Choosing α to be a primitive element shows that L is a splitting field of p_α, so L/L^G is normal, and thus finite Galois.

Finally, clearly $G \subset \mathrm{Gal}(L/L^G)$, and so

$$[L : L^G] \leq |G| \leq \left|\mathrm{Gal}(L/L^G)\right| = [L : L^G]$$

where the last step is because L/L^G is Galois, and thus G must be the full Galois group. □

1.5 Addendum: Separability

We have already had a somewhat detailed look into separability; in fact, there is some more we can say now that we know about the separable closure. We begin by defining the 'opposite' of a separable extension:

Definition 1.5.1 Let L/K be an algebraic extension. L/K is *purely inseparable* if for each $\alpha \in L$, either $\alpha \in K$ or the minimal polynomial of α over K is inseparable.

Lemma 1.5.2 *Let K be a field of characteristic $p > 0$. If $f \in K[x]$ is irreducible and inseparable, there is an irreducible separable polynomial $g \in K[x]$ such that $g(x^{p^n}) = f(x)$ for some $n \geq 0$.*

Proof If f is any irreducible inseparable polynomial, then f' shares a common factor with f so $f' = 0$. It follows that f is of the form

$$f(x) = x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0 = g(x^p)$$

where $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Note that if $h \mid g$, then $h(x^p) \mid f(x)$, so $\deg h(x^p) = 0$, i.e. g is irreducible.

Now let us prove the claim by induction on $\deg f \geq 1$. When it is degree one this is vacuously true since f cannot inseparable. In general, writing $f(x) = g(x^p)$, either g is separable and we are done, or it is an inseparable irreducible polynomial with $\deg g < \deg f$. By induction, $g(x) = h(x^{p^n})$ for h separable irreducible, thus $f(x) = h(x^{p^{n+1}})$. □

Purely inseparable extensions are important because we can break up any algebraic extension into a separable one and an inseparable one. The lemma governs the structure of these extensions.

Proposition 1.5.3 *Let L/K be an proper algebraic extension. The following are equivalent:*

(i) *L/K is purely inseparable.*

(ii) $\operatorname{char} K = p > 0$, *and for each $\alpha \in L$ there exists n such that $\alpha^{p^n} \in K$.*

(iii) $\operatorname{char} K = p > 0$, *and for each $\alpha \in L$ the minimal polynomial is of the form $x^{p^n} - a \in K[x]$.*

(iv) *For each $\alpha \in L$, the only conjugate of α is itself.*

(v) *If $\overline{K} \supset L \supset K$ is an algebraic closure, the only map $L \to \overline{K}$ over K is the inclusion.*

Proof *(i)* $\Rightarrow$ *(ii)* Since $K \subsetneq L$, the extension contains inseparable elements so $\operatorname{char} K = p > 0$. If $\alpha \in K$ already then the statement is trivial, so assume $\alpha \notin K$ and let f be its minimal polynomial. By the lemma, there is an irreducible separable $g \in K[x]$ such that $g(x^{p^n}) = f(x)$. Therefore g is monic and has α^{p^n} as a root, i.e. it is the minimal polynomial. So α^{p^n} is a separable element, and hence must lie in K.

(ii) $\Rightarrow$ *(iii)* We know $\alpha^{p^n} \in K$, so

$$f(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n} \in K[x].$$

Let $\deg \alpha = k \leq p^n$, and so the minimal polynomial is $(x - \alpha)^k$; observe that any monic irreducible factor (over K) of $f(x)$ has α as a root, and hence must divide (so must be) $(x - \alpha)^k$. Therefore $f(x)$ is a power of $(x - \alpha)^k$, so $k \mid p^n$ i.e. k is a prime power.

$(iii) \Rightarrow (iv)$ This implies $a = \alpha^{p^n}$, so the minimal polynomial is

$$x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n},$$

and hence it has only one root, namely α itself.

$(iv) \Rightarrow (v)$ Let $\sigma\colon L \to \overline{K}$ be a map over K, and assume $\alpha \in L \setminus K$. If we consider the restriction $\sigma\colon K(\alpha) \to L$, we know α must map to one of its conjugates, hence $\alpha \mapsto \alpha$. On the other hand if $\alpha \in K$, then it is fixed by definition, so σ is the inclusion.

$(v) \Rightarrow (i)$ If L/K wasn't purely inseparable, there would be some $\alpha \in L \setminus K$ which is separable. Then $\deg \alpha \geq 2$, so α has at least one conjugate $\beta \in \overline{K}$ with $\beta \neq \alpha$. By Cor. 1.2.11 applied to the algebraic closure, there is an automorphism $\sigma\colon \overline{K} \to \overline{K}$ over K sending $\alpha \mapsto \beta$, so restricting to L gives a nontrivial map $L \to \overline{K}$ over K. This is the desired contradiction. □

Example 1.5.4 Let k be any field of characteristic $p > 0$, write $K = k(t)$ for the field of rational functions, and take $L = K(t^{1/p})$. Note that $\alpha = t^{1/p}$ is algebraic as a root of $x^p - t \in K[x]$, so L is a well-defined proper algebraic extension. But any element of L, of the form $f(t^{1/p})$ for $f(x) \in K[x]$, would have its pth power in K by the Frobenius, so by the previous proposition this is a purely inseparable extension. (Note that $t^{1/p} \notin K$, because if so then $tg(t)^p = f(t)^p$ for some polynomials $f, g \in k[t]$ which is impossible since the degree of the LHS is 1 and of the RHS is 0, mod p.)

Remark 1.5.5 Even though in a purely inseparable extension, elements have no nontrivial conjugates, it is not true that an inseparable irreducible polynomial has only one root. For example, take $K = \mathbb{F}_p(t)$ and $n \nmid p$. Then $f(x) = x^{pn} - t \in K[x]$ is obviously inseparable. As a polynomial with coefficients in $\mathbb{F}_p[t]$, t divides the constant term and not the leading term, and $t^2 \nmid t$. Hence f is irreducible over $\mathbb{F}_p[t]$, and thus over K too by Gauss' lemma. But $x^n - 1$ has n distinct roots, so if α is any root of $f(x)$, then $\zeta\alpha$ are also roots for the distinct roots ζ of $x^n - 1$.

Now let L/K be an arbitrary algebraic extension, and recall that L_{sep} denotes the separable closure, i.e. the subfield of L consisting of separable elements over K. We have a tower $K \subset L_{\text{sep}} \subset L$; by definition L_{sep}/K is separable. In fact L/L_{sep} is purely inseparable.

Indeed, if $\alpha \in L$ but not L_{sep}, then the minimal polynomial p_α over K is irreducible and inseparable, so $p_\alpha(x) = g(x^{p^n})$ for g separable and irreducible over K. We know α^{p^n} satisfies g, so α^{p^n} is separable over K, hence is contained in L_{sep}. By our equivalent conditions, this shows L/L_{sep} is purely inseparable.

Definition 1.5.6 Let L/K be a finite extension. The number $[L_{\text{sep}} : K]$ is called the *separable degree* of L/K, and we write

$$[L : K]_{\text{sep}} = [L_{\text{sep}} : K].$$

Evidently this divides $[L : K]$, and we will sometimes call the quotient $[L : L_{\text{sep}}]$ the *inseparable degree*.

So, of course, $[L : K]_{\text{sep}} = [L : K]$ if and only if L/K is separable. Similarly, if $[L : K]_{\text{sep}} = 1$ then $K = L_{\text{sep}}$ so L/K is purely inseparable, and conversely if L/K is purely inseparable then $L_{\text{sep}} = K$ so $[L : K]_{\text{sep}} = 1$. Let us give an alternative and more useful interpretation of the separable degree now. If L/K is finite and $F \supset K$, we will write $\#\{L/K \to F/K\}$ for the number of maps $L \to F$ over K. Note that if $F = \overline{K}$ is an algebraic closure containing L, then by Lemma 1.4.1 this number is finite.

Lemma 1.5.7 *Suppose $K \subset L \subset F$ are finite extensions contained in an algebraic closure $\overline{K}$. Then*

$$\#\{F/K \to \overline{K}/K\} = \#\{L/K \to \overline{K}/K\} \cdot \#\{F/L \to \overline{K}/L\}.$$

Proof Fix $\sigma\colon L \to \overline{K}$ over K, and by Cor. 1.2.12 we can extend this to an automorphism $\widetilde{\sigma}\colon \overline{K} \to \overline{K}$. We claim post-composition with $\widetilde{\sigma}$ induces a bijection

$$\text{Hom}_L(F, \overline{K}) \xrightarrow{\sim} \{\tau\colon F/K \to \overline{K}/K : \tau|_L = \sigma\}.$$

Indeed if $\tau\colon F \to \overline{K}$ fixes L, then $\sigma \circ \tau$ fixes K and sends $\alpha \in L$, to $\sigma(\alpha)$. Conversely, if $\tau\colon F \to \overline{K}$ is over K and restricts to σ, then $\sigma^{-1}\tau$ fixes L and is mapped to τ, proving the claim. To finish, observe than any map $F \to \overline{K}$ over K is determined by its restriction to L, and then a map extending that restriction. Therefore:

$$\begin{aligned}\#\{F/K \to \overline{K}/K\} &= \sum_{\sigma \in \text{Hom}_K(L,\overline{K})} \#\{\tau\colon F/K \to \overline{K}/K : \tau|_L = \sigma\} \\ &= \sum_{\sigma \in \text{Hom}_K(L,\overline{K})} \#\{F/L \to \overline{K}/L\},\end{aligned}$$

which follows from the bijection we just constructed, and it completes the proof since the cardinality of the set we sum over is $\#\{L/K \to \overline{K}/K\}$. □

Corollary 1.5.8 *Let L/K and F/L be finite extensions.*

1. *If $\overline{K}$ is an algebraic closure containing L, then $[L/K]_{\text{sep}} = \#\{L/K \to \overline{K}/K\}$. In particular it is independent of the choice of $\overline{K}$.*
2. *We have the formula $[F : K]_{\text{sep}} = [F : L]_{\text{sep}}[L : K]_{\text{sep}}$.*
3. *F/K is separable if and only if F/L and L/K are separable. Similarly F/K is purely inseparable if and only if F/L and L/K are purely inseparable.*

Proof (1) We know by the previous lemma that

$$\#\{L/K \to \overline{K}/K\} = \#\{L_{\text{sep}}/K \to \overline{K}/L\}\#\{L/L_{\text{sep}} \to \overline{K}/L_{\text{sep}}\}.$$

Since L/L_{sep} is purely inseparable, Prop. 1.5.3(v) shows that the right-most number is 1. Since L_{sep}/K is separable, Lemma 1.4.1 shows that the middle number is $[L_{\text{sep}} : K] = [L : K]_{\text{sep}}$, which is what we wanted.

(2) follows from (1) and the lemma. For (3), if F/L and L/K are separable (resp. purely inseparable), then their separable degrees are their degrees (resp. 1), so by (2) the separable degree of F/K is its degree (resp. 1). Conversely, if F/K has separable degree 1 then the two intermediate degrees also do. Similarly, if $[F : K]_{\text{sep}} = [F : K]$, then since $[F : L]_{\text{sep}} \leq [F : L]$ and $[L : K]_{\text{sep}} \leq [L : K]$, (2) implies equality. □

The biggest takeaway from this result is the transitivity of separability: If we want to show a finite extension L/K is separable, then we can split it up into smaller extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

and show that each K_{i+1}/K_i is separable. We also remark that this extends easily to arbitrary algebraic extensions. If L/K and F/L are (possibly infinite) separable, we claim F/K is separable. Indeed, if $\alpha \in F$ then let $\{\beta_1, \ldots, \beta_n\}$ be the coefficients of its minimal polynomial over L. Consider:

$$\begin{array}{ccccc} K & \twoheadrightarrow & L & \twoheadrightarrow & F \\ \downarrow & \nearrow & & \nearrow & \\ K(\beta_1, \ldots, \beta_n) & \longrightarrow & K(\beta_1, \ldots, \beta_n, \alpha) & & \end{array}$$

If p_α is the minimal polynomial over L, we know α has the same minimal polynomial over $K(\beta_1, \ldots, \beta_n)$, so $K(\underline{\beta}, \alpha)/K(\underline{\beta})$ is generated by a separable element and thus is separable. For the same reason $K(\underline{\beta})/K$ is separable. These are finite, and so α is separable over K.

As a final observation, we can prove that any finite purely inseparable extension L/K in characteristic p has degree a power of p. Indeed, we can split it up into simple extensions

$$K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = L,$$

and by the corollary each extension is purely inseparable. Since the minimal polynomial of each α_i over the $(i-1)$th extension is of the form $x^{p^n} - a$, each extension is degree a power of n. Hence the overall one is. So:

Proposition 1.5.9 *For any finite extension L/K, the inseparable degree $[L : K]_{\text{in}}$ is either 1 or a power of* $\operatorname{char} K$. *In particular,* $\operatorname{char} K$ *divides the degree of any inseparable extension.*

2 Galois Theory

2.1 The Fundamental Theorem

We now prove the central result about the Galois extensions that we defined in the previous section. Because of the work we have already done, it will not be too difficult. From here on, 'Galois extension' will mean 'finite Galois extension'. The theorem is as follows:

Theorem 2.1.1 *Let L/K be a finite Galois extension. The maps given by*

$$\begin{Bmatrix}\text{intermediate extensions } F \\ \text{s.t. } L \supset F \supset K\end{Bmatrix} \underset{L^H \longleftarrow\!\shortmid\, H}{\overset{F \longmapsto \mathrm{Gal}(L/F)}{\rightleftarrows}} \begin{Bmatrix}\text{subgroups } H \\ \text{of } \mathrm{Gal}(L/K)\end{Bmatrix}$$

form order-reversing mutually inverse bijections with L corresponding to $\{1\}$ and K corresponding to $\mathrm{Gal}(L/K)$. A subextension F/K is normal if and only if $\mathrm{Gal}(L/K) \cdot F \subset F$, and the correspondence restricts to a bijection

$$\begin{Bmatrix}\text{normal extensions } F \\ \text{s.t. } L \supset F \supset K\end{Bmatrix} \longrightarrow \begin{Bmatrix}\text{normal subgroups } H \\ \text{of } \mathrm{Gal}(L/K)\end{Bmatrix}$$

between normal extensions and normal subgroups, and if $H \leq \mathrm{Gal}(L/K)$ is such a normal subgroup then the map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K) \qquad \sigma \mapsto \sigma|_{L^H}$$

is well-defined and surjective with kernel H. In particular, we have a natural isomorphism $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$.

Proof First, the 'order-reversing' part is trivial because if $F \subset F'$ are intermediate extensions, then any $\sigma\colon L \to L$ fixing F' also fixes F, so $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$. For the first part, we have to show the following two equalities:

$$L^{\mathrm{Gal}(L/F)} = F \qquad \mathrm{Gal}(L/L^H) = H.$$

The second was already proven (in more generality) in Thm. 1.4.10, and for the first observe that L/F is obviously separable, and it is normal too since if $\sigma\colon L \to \overline{K}$ fixes F then it also fixes K, so $\sigma(L) \subset L$ as L/K is normal (Prop. 1.4.3). Therefore L/F is Galois, so equivalently $L^{\mathrm{Gal}(L/F)} = F$ from Thm. 1.4.5.

Moving onto the second part, let $H \leq G = \mathrm{Gal}(L/K)$ be a normal subgroup and write $F = L^H$. We claim that any $\sigma \in G$ preserves F (i.e. $\sigma(F) \subset F$). Indeed, let $\alpha \in F$ and choose $\tau \in H$, so there exists $\tau' \in H$ such that $\tau\sigma = \sigma\tau'$ by normality. Now

$$\tau(\sigma(\alpha)) = \sigma(\tau'(\alpha)) = \sigma(\alpha),$$

so $\sigma(\alpha) \in L^H = F$ since $\tau \in H$ was arbitrary. This immediately implies that F/K is normal, because if $\overline{K} \to \overline{K}$ is a map fixing K, then it preserves L since

L/K is normal (and gives an automorphism), so it preserves F (and gives an automorphism). It follows that

$$\phi\colon G \to \mathrm{Gal}(F/K) \qquad \sigma \mapsto \sigma|_F$$

is well-defined, and clearly a group homomorphism. σ is in the kernel iff σ preserves F, i.e. $\sigma \in \mathrm{Gal}(L/F)$. By the first part of the theorem, $\ker\phi = \mathrm{Gal}(L/F) = H$. To see ϕ is surjective, we note that as F/K is Galois, the order of the codomain is

$$|\mathrm{Gal}(F/K)| = [F:K] = [L:K]/[L:F] = |G|\,/\,|H| = |G/H|\,,$$

where in the penultimate step we used that L/F was Galois, as we already know from before. But the image of ϕ is isomorphic to G/H, so this shows the image is all of $\mathrm{Gal}(F/K)$.

All that remains is to show that the corresponding subgroup of a normal extension F/K is a normal subgroup. Let $H = \mathrm{Gal}(L/K) \in G$ and let $\sigma \in G$, $\tau \in H$. Since F is the fixed field of H, it suffices to show that $\sigma^{-1}\tau\sigma$ fixes F. But since F/K is normal, $\sigma|_F\colon F \to L \hookrightarrow \overline{K}$ has image in F, so σ preserves F. Therefore if $\alpha \in F$ then

$$\sigma^{-1}(\tau(\sigma(\alpha)) = \sigma^{-1}\sigma(\alpha) = \alpha,$$

because $\sigma(\alpha) \in F$ and τ fixes F. Since α was arbitrary, $\sigma^{-1}\tau\sigma \in H$ because it fixes F. □

We must stress that we didn't actually do anything in this proof. Most of the work had been done in Thm. 1.4.5 and Thm. 1.4.10. We refer to this result as the *Galois correspondence*, and it is the basis for most interesting results of Galois theory.

Let us now move onto some examples. An easy way to generate Galois extensions is to use Thm. 1.4.10: with this we can take any finite group G which acts faithfully (by automorphisms) on a field L, and get a Galois extension L/L^G with Galois group G.

Example 2.1.2 (every group is a Galois group) Let k be a field and set $L = k(x_1, \ldots, x_n)$ to be rational functions in n variables. The symmetric group S_n acts on L by permuting the free variables, and of course only $() \in S_n$ acts trivially so it is a faithful action. From algebra it is well known that

$$K \coloneqq L^{S_n} = k(e_1, \ldots, e_n)$$

where the $\{e_i\}$ are the elementary symmetric polynomials. Then L/K has Galois group S^n so is a degree $n!$ extension. Then $A_n \leq S_n$ is normal, so the fixed field of A_n is a degree 2 normal extension of K. Now, let G be any group of order n, then G acts faithfully on itself by left multiplication, so $G \hookrightarrow S_n$ is a subgroup. Hence the fixed L-subfield of G gives a Galois extension L/L^G with Galois group G.

Remark 2.1.3 Let $f \in K[x]$ be a separable polynomial. We will sometimes say loosely that the 'Galois group of f' (usually when f is irreducible) the Galois group of a splitting field L of f. Now, a splitting field of any polynomial of degree n has at degree at most $n!$, because if $\{\alpha_1, \ldots, \alpha_n\}$ are the roots then

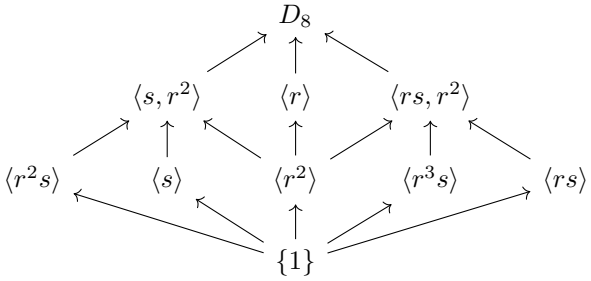
$$[L : K] = [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots ,$$

and each time we adjoin a root α_i the polynomial can be divided by $x - \alpha_i$, so the expression is $\leq n(n-1)\cdots = n!$. There is a Galois-theoretic interpretation of this fact: On one hand the Galois group of f must permute the roots of f, and on the other hand those roots generate L, so each $\sigma \in \mathrm{Gal}(L/K)$ is determined by this permutation. Hence $\mathrm{Gal}(L/K) \subset S_n$. Remember that every Galois extension is a splitting field of a separable polynomial, so one should always think of $\mathrm{Gal}(L/K)$ as a subgroup of permutations subject to some conditions.

Example 2.1.4 Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, and write $\alpha = 2^{1/4} \in \mathbb{R}$. The four roots of f over $\mathbb{C}$ are $\pm\alpha, \pm i\alpha$, and no products of the corresponding linear factors are in $\mathbb{Q}[x]$, so its irreducible (and separable). The splitting field is

$$L = \mathbb{Q}(\alpha, i) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q},$$

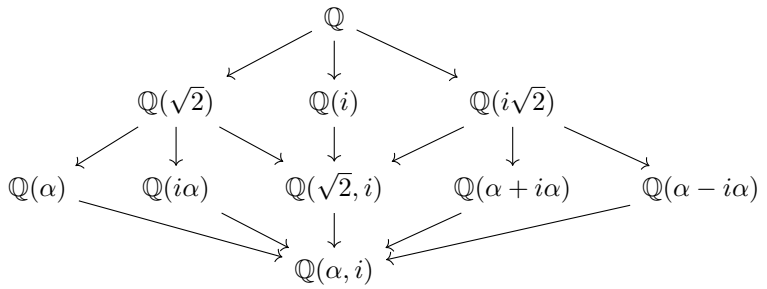
and $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree 4 because its minimal polynomial is f; on the other hand we know $\mathbb{Q}(\alpha, i)/\mathbb{Q}(\alpha)$ is not degree 1 and is at most degree 2; hence $L/\mathbb{Q}$ has degree 8. Visualize the four roots in the complex plane, then we view $G = \mathrm{Gal}(L/\mathbb{Q})$ as a subgroup of S_4, the permutations of the points. If $\sigma \in G$, then $\sigma(-x) = -\sigma(x)$, so any permutation has both diagonals of the resulting square as lines of symmetry. Hence $G \leq D_8 \leq S_4$ so $G = D_8 = \langle s, r \rangle$ where s is reflection and r is rotation. This is the subgroup lattice of D_8:



Here, the top row is order 8, second is order 4, and third is order 2. Let us use this to compute all of the intermediate subfields of $\mathbb{Q}(\alpha, i)$. From our square, $r(\alpha) = i\alpha$ and $s(\alpha) = -\alpha$. These imply that $r(\sqrt{2}) = -\sqrt{2}$, and $s(\sqrt{2}) = \sqrt{2}$. In addition, the square tells us that $r(i\alpha) = -\alpha$ and s fixes $i\alpha$; also $2i = i\alpha^4 = (i\alpha)\alpha^3$, so

$$2r(i) = (-\alpha)(i\alpha)^3 = 2i \qquad 2s(i) = (i\alpha)(-\alpha)^3 = -2i,$$

i.e. $r(i) = i$ and $s(i) = -i$. We will show that the subfield lattice is



We know the top and bottom already; each of the subgroup inclusions in previous diagrams has index 2, so all extensions have degree 2. Begin with the second row: $r^2(\sqrt{2}) = \sqrt{2}$ and s also fixes it, so $L^{\langle s, r^2\rangle} \supset \mathbb{Q}(\sqrt{2})$, but this is a degree two extension so we have equality. Similarly, r fixes i so $i \in L^{\langle r\rangle}$, but for degree reasons it is $\mathbb{Q}(i)$. Likewise, $i\sqrt{2}$ is fixed by rs and r^2 but is the root of $x^2 + 2 \in \mathbb{Q}[x]$.

Onto the third row: $r^2 s(\alpha) = r^2(-\alpha) = \alpha$, $\mathbb{Q}(\alpha) \subset L^{\langle r^2 s\rangle}$, but $\alpha \notin \mathbb{Q}(\sqrt{2})$ (so $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \geq 2$), because α is not fixed by s. The same reasoning shows $L^{\langle s\rangle} = \mathbb{Q}(i\alpha)$. For $L^{\langle r^2\rangle}$, we already know that $\sqrt{2}, i$ are contained; on the other hand

$$\mathbb{Q}(\sqrt{2}, i) \subset L^{\langle r^2\rangle} \subset L$$

and $L/\mathbb{Q}(\sqrt{2}, i)$ has at most degree 2 and $L/L^{\langle r^2\rangle}$ has exactly degree 2. For the last two extensions, observe $r^3 s = sr$, so we will take as a guess $(1 + sr)\alpha = \alpha + i\alpha$ which is fixed by sr. Note that $r^2(\alpha + i\alpha) = -(\alpha + i\alpha)$ so it is not contained in $\mathbb{Q}(i\sqrt{2})$, so we're done. The same thing using rs shows that the last extension is $\mathbb{Q}(\alpha - i\alpha)$.

The example demonstrates the utility of Galois groups, in that we were able to transfer the problem into one about elementary group theory. Finally, all of these extensions are finite separable so let us attempt to find primitive elements for $\mathbb{Q}(\sqrt{2}, i)$ and $\mathbb{Q}(\alpha, i)$. An element is primitive iff no elements outside of the corresponding group fixes it. E.g., considering $\alpha + i$, $r(\alpha + i) = i\alpha + i \neq \alpha + i$ and $s(\alpha + i) = -(\alpha + i) \neq \alpha + i$. Hence $\mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha + i)$. Similarly, $\sqrt{2} + i$ generates $\mathbb{Q}(\sqrt{2}, i)$.

In what follows we will look at lots of Galois extensions, so let us introduce some generalities to make it easier. Let $L, M \subset F$ be subfields. We define $LM \subset$ called the *composite field* to be the intersection of all subfields of F containing both L and M (so in particular contain L and M). Suppose $K \subset L \cap M$, and that $L = K(S)$ and $M = K(S')$ for some generating sets S, S'. Then $LM = K(S \cup S')$, as this is a field containing L and M which is contained in every other one.

Sometimes, if L, M are extensions of K we write LM without reference to the containing field; this is done especially when they are algebraic, and subfields of some algebraic closure $\overline{K}$.

Lemma 2.1.5 *Let $K \subset L, M \subset \bar{K}$ with L, M finite over K. Then*

$$[LM : L] \leq [M : K] \quad \textit{and} \quad [LM : M] \leq [L : K].$$

In particular

$$[LM : K] \leq [M : K][L : K].$$

Proof The second part follows immediately because

$$[M : K][L : K] \geq [LM : L][L : K] = [LM : K].$$

Now we prove the first part of the first statement, and the second follows by symmetry. Write $L = K(\underline{\alpha})$ and $M = K(\underline{\beta})$ where this is shorthand for e.g. $(\underline{\alpha}) = (\alpha_1, \ldots, \alpha_m)$. Now we have parallel sequences:

$$\begin{aligned} L = K(\underline{\alpha}) \subset K(\underline{\alpha}, \beta_1) \subset \cdots \subset K(\underline{\alpha}, \beta_1, \ldots, \beta_n) = LM \\ K \subset (\beta_1) \subset \cdots \subset K(\beta_1, \ldots, \beta_n) = M \end{aligned}$$

We claim (which suffices by the degree product formula) that

$$[K(\underline{\alpha}, \beta_1, \ldots, \beta_{i+1}) : K(\underline{\alpha}, \beta_1, \ldots, \beta_i)] \leq [K(\beta_1, \ldots, \beta_{i+1}) : K(\beta_1, \ldots, \beta_i)].$$

But indeed this is obvious because the minimal polynomial of β_{i+1} over $K(\beta_1, \ldots, \beta_i)$ is contained in $K(\underline{\alpha}, \beta_1, \ldots, \beta_i)[x]$, and so it divides the minimal polynomial of β_{i+1} over this latter field. □

Another easy but useful lemma is the following one:

Lemma 2.1.6 *Let L, M be extensions of K (contained in some $\overline{K}$). If L and M are normal (resp. separable, or Galois) then LM is normal (resp. separable, or Galois).*

Proof The statement about separability follows from the fact that LM is generated over K by generators of L and M, and Galois follows from that, finiteness, and normality. So, suppose L is the splitting field of $\{f_i\}$ and M is the splitting field of $\{g_j\}$; we claim LM is the splitting field of $\{f_i\} \cup \{g_j\}$. Clearly each of these polynomials splits in LM, and LM is generated by generators of L and M, i.e. roots of the f_i and g_j. □

Let us briefly discuss extensions of finite fields and containments. Let p be prime, fix $\overline{\mathbb{F}_p}$, and let $q = p^n$. We already know $\mathbb{F}_q/\mathbb{F}_p$ is Galois and has Galois group $\langle\sigma\rangle$ cyclic of order n, where $\sigma = (-)^p$. Suppose $m \mid n$ and write $mk = n$. Since $x - 1 \mid x^k - 1$, $p^m - 1 \mid p^n - 1$. Therefore

$$\alpha \in \mathbb{F}_{p^m} \Rightarrow \alpha^{p^m - 1} = 1 \Rightarrow \alpha^{p^n - 1} = 1 \Rightarrow \alpha \in \mathbb{F}_{p^n},$$

because $\mathbb{F}_{p^n}$ is the set of roots of $x^{p^n} - x$ in $\overline{F_p}$. So $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ is an intermediate extension. On the other hand, every subgroup of $\langle\sigma\rangle$ is of the form $m\mathbb{Z}/n\mathbb{Z} = \langle\sigma^m\rangle$ of order k. The corresponding fixed field

$$L = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^m} = \alpha\} = \mathbb{F}_{p^m}.$$

This gives a canonical bijection

$$\{m : m \mid n\} \xrightarrow{\sim} \left\{\text{subfields of } \mathbb{F}_{p^n}\right\}$$

given by $m \mapsto \mathbb{F}_{p^m}$. It also tells us what *all* extensions of finite fields are and their Galois groups. Namely if $\mathbb{F}_{q_1}/\mathbb{F}_{q_0}$ is such an extension, then both fields have the same characteristic p and hence must have q_1 and q_0 powers of p. Then $\mathbb{F}_{q_0}$ is intermediate to $\mathbb{F}_{q_1}/\mathbb{F}_p$ which is Galois, thus $q_0 = p^m$ and $q_1 = p^n$ where $m \mid n$. Moreover, $\mathrm{Gal}(\mathbb{F}_{q_1}/\mathbb{F}_{q_0})$ is just the corresponding subgroup $\langle\sigma^m\rangle$ and has degree $k = n/m$. Here's a concrete example.

Example 2.1.7 Take $n = 4$ and $p = 2$; we claim $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. Indeed $f(0), f(1) \neq 0$, and

$$f(x) = (x^2 + x + 1)(x^2 + x) + 1,$$

where x^2+x+1 is the only irreducible polynomial of degree 2 (so f doesn't have irreducible factors of degree 1 or 2). Thus viewing $\mathbb{F}_{16}/\mathbb{F}_2$ as a four dimensional vector space we can write

$$\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \{a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 : a_i \in \mathbb{F}_2\}$$

where multiplication is subject to the relation $\alpha^4 = \alpha + 1$. Now $16 = 2^4$, so the subfields are $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$; let us compute $\mathbb{F}_4 = \{\beta : \beta^4 = \beta\}$. We have 0 and 1, and we can compute that $(\alpha^2 + \alpha + 1)^4 = \alpha^2 + \alpha + 1$, and its square is $\alpha + \alpha^2$, so

$$\mathbb{F}_4 = \{0, 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha\} \subset \mathbb{F}_{16}.$$

2.2 Basic Examples

In general, Galois theory will help us convert problems about field extensions to those about finite groups and sometimes number theory or algebra. One such problem which we have previously assumed (but not relied on for anything) is the fundamental theorem of algebra:

Theorem 2.2.1 $\mathbb{C}$ *is algebraically closed.*

This is both an algebraic statement and an analysis statement; after a trivial fact about the completeness of $\mathbb{R}$, we will see that the algebraic analog is:

Proposition 2.2.2 *Suppose G is a finite group of even order such that all proper subgroups have even index. Then the only subgroup H without any subgroups of index 2 is trivial.*

This is very easy using the following lemma from group theory:

Lemma 2.2.3 *Any nontrivial p-group has a subgroup of index p.*

Proof Let $|G| = p^n$ and induct on n; when $n = 1$ take $\{e\}$. Otherwise, G has nontrivial center Z, which is also a p-group, so it has a subgroup $H \leq Z$ of order p by Cauchy's theorem. Then H is normal in G, and G/H is a p-group of order p^{n-1}, so it has an index p subgroup which we can write $K/H \leq G/H$ for some $K \leq H$. Then $[G : K] = [G/H : K/H] = p$. □

Proof (of Prop. 2.2.2) Let $K \leq G$ be a Sylow-2 subgroup, so $2 \nmid [G : K]$ hence $K = G$ so G is a 2-group of some order 2^k, and thus $|H| = 2^l$. If $l \neq 0$ then by Lemma 2.2.3 H has an index 2 subgroup which cannot be, so $l = 0$ and H is trivial. □

To explain why this the algebraic version of the fundamental theorem of algebra, we use the following two facts:

Lemma 2.2.4

1. *Any polynomial $f \in \mathbb{R}[x]$ of odd degree has a real root.*
2. *$\mathbb{C}$ has no extensions of degree 2.*

Proof For (1), we may assume f is monic of degree n, then $\lim_{x\to\pm\infty} f(x)/x^n = 1$, so there are $x_+ > x_-$ in $\mathbb{R}$ such that $f(x_-) < 0 < f(x_+)$. Hence some $x \in [x_-, x_+]$ is a real root of f. For (2), if there was such an extension then it would be generated by any element outside of $\mathbb{C}$, say α, satisfying $\alpha^2 + z\alpha + w = 0$ with $z, w \in \mathbb{C}$. But this is solved via the quadratic equation, and $\mathbb{C}$ is closed under square roots since $re^{i\theta}$ has square roots $\pm\sqrt{r}e^{i\theta/2}$. □

Proof (of Thm. 2.2.1) It suffices to show that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, i.e. $\mathbb{C}$ is a splitting field of the set $\mathbb{R}[x]$. It is generated by roots of polynomials in that set (i.e. $x^2 + 1$), so we need to show any $f \in \mathbb{R}$ splits over $\mathbb{C}$. It suffices to assume that f is monic, irreducible, and thus of even degree. Let $\alpha \in \overline{C}$ be a root, and write L for the normal closure of the extension $\mathbb{C}(\alpha)/\mathbb{R}$, so $L/\mathbb{R}$ is Galois.

If $\mathbb{R} \subsetneq F \subset L$, then $F/\mathbb{R}$ has even degree; indeed take any $\beta \in F$ not in $\mathbb{R}$, then its minimal polynomial must be even since it is irreducible over $\mathbb{R}$. This means that $\mathrm{Gal}(L/\mathbb{R})$ has even order and has proper subgroups of even index only. Letting $H = \mathrm{Gal}(L/\mathbb{C})$, if $K \leq H$ had index two then $L^K/\mathbb{C}$ would have index 2, so no such K exists. Therefore by Prop. 2.2.2, H is trivial, hence $\mathbb{C} = L^H = L$, thus $\alpha \in \mathbb{C}$. □

This proof is likely a minimal element of the set of proofs of the fundamental theorem of algebra totally ordered by amount of analysis used. Of course, it is not 'trivial' because we have used the Sylow theorems twice, but all of that is purely algebraic. This is also slightly more general; we could have taken any

field F in characteristic 0 with the property that all polynomials of odd degree have a root, and that the splitting field of $\{f \in F[x] : \deg f = 2\}$ is a finite extension of F. Then that splitting field is an algebraic closure of F.

As our next example, let us try to understand the pth roots of unity over $\mathbb{Q}$ for a prime p. We will do this in much more generality in Sec. 2.4, but this is the simplest case of a *cyclotomic extension*.

A pth root of unity over $\mathbb{Q}$ is an element α of some extension, which we can fix to be in $\overline{\mathbb{Q}} \subset \mathbb{C}$, such that $\alpha^n = 1$. 1 is trivially a pth root of unity, so we have the factorization

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

We will write $\Phi_p = x^{p-1} + \cdots + x + 1$ and call its roots as elements of $\mathbb{C}$ the *primitive pth roots of unity*. If we write $1 = e^{2\pi i}$, then it is clear that the pth roots are of the form $e^{\frac{1}{p}2\pi i}, e^{\frac{2}{p}2\pi i}, \ldots$, which graphically go around the complex unit circle (in particular are all clearly distinct). Writing, $\zeta_p = \zeta = e^{2\pi i/p}$, the set of primitive pth roots is

$$\{\zeta^1, \zeta^2, \ldots, \zeta^{p-1}\}.$$

Hence $\mathbb{Q}(\zeta)$ contains all the roots of $x^p - 1$ and is its splitting field, so $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois. Any element σ of the Galois group is determined by $\sigma(\zeta) = \zeta^i$ for a unique $0 < i < p$; σ corresponds to i and τ to j, then

$$\sigma\tau(\zeta) = \sigma(\zeta^j) = (\zeta^i)^j = \zeta^{ij},$$

so $\sigma\tau$ corresponds to $ij \pmod p$. Thus $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \subset (\mathbb{Z}/p\mathbb{Z})^\times$. To show this is an equality, we show $\Phi_p(x) \in \mathbb{Q}[x]$ is irreducible, which shows that the Galois group has order $p-1$, as does $(\mathbb{Z}/p\mathbb{Z})^\times$. It suffices to show $\Phi(x+1)$ is irreducible; this satisfies $(x+1)^p - 1 = x\Phi_p(x+1)$, so modulo p we see

$$x\Phi_p(x+1) \equiv x^p + 1 - 1 = x^p \Rightarrow \Phi_p(x+1) \equiv x^{p-1} \pmod p,$$

so p doesn't divide the top degree coefficient and does divide all the others. In addition, evaluating $\Phi_p(x+1)$ at $x = 0$ gives $\Phi_p(1) = p$, so p^2 doesn't divide the constant term. Hence by Eisenstein's criterion, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$, and hence so is $\Phi_p \in \mathbb{Q}[x]$. We have shown:

Proposition 2.2.5 *Let p be a prime and $\zeta_p = e^{2\pi i/p}$. Then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a splitting field for $\Phi_p(x)$ containing all the pth roots of unity. $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension of degree $p-1$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$ given by sending $\zeta_p \mapsto \zeta_p^i$ for $i \in (\mathbb{Z}/p\mathbb{Z})^\times$.*

One way these extensions are helpful is in understanding the numbers $\cos(2\pi/p) \in \mathbb{R}$, e.g. we could ask whether it is rational, and if not what its minimal polynomial over $\mathbb{Q}$ is.

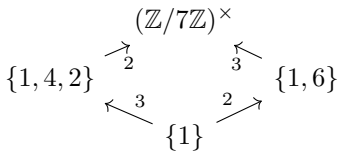
Let us do an example with $p = 7$; set $\omega = 2\cos(2\pi/7)$, then clearly $\omega = \zeta + \zeta^{-1}$. Observe that $\omega^2 = \zeta^2 + \zeta^{-2} + 2$ and $\omega^3 = \zeta^3 + \zeta^{-3} + 3\zeta + 3\zeta^{-1} = \zeta^3 + \zeta^{-3} + 3\omega$. But now notice that

$$\begin{aligned} 0 = 1 + \zeta + \zeta^2 + \cdots &= 1 + \omega + (\zeta^2 + \zeta^{-2}) + (\zeta^3 + \zeta^{-3}) \\ &= 1 + \omega + (\omega^2 - 2) + (\omega^3 - 3\omega), \end{aligned}$$

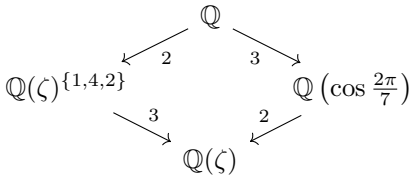
so $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ has ω as a root. On the other hand, if f is not irreducible then it has a rational root p/q, but then $p \mid 1$ and $q \mid 1$, so it would be ± 1, but $f(\pm 1) \neq 0$. Hence $\mathbb{Q}(\omega)/\mathbb{Q}$ has degree 3 with minimal polynomial f. Obviously $\mathbb{Q}(\omega) = \mathbb{Q}(\cos(2\pi/7))$, so the polynomial

$$f(2x)/8 = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8}$$

is the minimal polynomial of $\cos(2\pi/7)$ over $\mathbb{Q}$. Let us try to write down all intermediate extensions of $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. The group part is easy:



This is just using that $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic of order 6 with generator, say, 5. Now, $\{1, 6\} = \{\pm 1\}$, and this group fixes the element $\sigma_1(\zeta) + \sigma_{-1}(\zeta) = \zeta + \zeta^{-1} = \omega$ from before, so we can write the corresponding extension as $\mathbb{Q}(\cos(2\pi/7))$. Observe also that the automorphism is complex conjugation, so this extension is equal to $\mathbb{Q}(\zeta) \cap \mathbb{R}$.



It remains to determine $L = \mathbb{Q}(\zeta)^{\{1,4,2\}}$. We know summing over the conjugates gives an element:

$$\alpha \coloneqq \zeta + \zeta^4 + \zeta^2 \in L.$$

α will generate L as long as it isn't in $\mathbb{Q}$; let's determine α. Since its degree 2, it has a degree two polynomial; notice that

$$\alpha^2 = \zeta^2 + 2\zeta^3 + 2\zeta^5 + \zeta^6 + \zeta = \zeta^3 + \zeta^6 + \zeta^5 - 1$$

using $\Phi_7(\zeta) = 0$. But then $\alpha^2 + 2 + \alpha = 0$, so $\alpha = (-1 \pm \sqrt{-7})/2$. Therefore $L = \mathbb{Q}(i\sqrt{7})$ is the remaining extension, which would actually be somewhat difficult to guess without Galois theory.

Later on we will be able to use Galois theory to find a more 'closed form' solution for $\omega = \zeta + \zeta^{-1}$. Here's a preview: First observe that we already know what the conjugates of ω are. The Galois group of $\mathbb{Q}(\omega)/\mathbb{Q}$ is the quotient consisting of cosets

$$\big\{\{\pm 1\}, \{\pm 2\}, \{\pm 3\}\big\},$$

and therefore the other roots of $x^3 + x^2 - 2x - 1$ are

$$\omega_2 = \zeta^2 + \zeta^{-2} \qquad \omega_3 = \zeta^3 + \zeta^{-3}.$$

Since its a cubic equation, we want to solve it in terms of square and cube roots; the trick will be to use the normal extension $\mathbb{Q}(\omega, \zeta_3)/\mathbb{Q}(\zeta_3)$. Notice that $\mathbb{Q}(\omega, \zeta_3) = \mathbb{Q}(\omega)\mathbb{Q}(\zeta_3)$ has degree divisible by 2 and 3 and less then 6, hence it is degree 6, so $\mathbb{Q}(\omega, \zeta_3)/\mathbb{Q}(\zeta_3)$ has order 3 with the same irreducible polynomial $x^3 + x^2 - 2x - 1$. The next trick is to consider the element

$$\alpha = \omega + \zeta_3\omega_2 + \zeta_3^2\omega_3 \in \mathbb{Q}(\omega, \zeta_3).$$

if σ is the generator of the Galois group sending $\omega \mapsto \omega_2$, then $\sigma(\alpha) = \zeta_3^2\alpha$, so α^3 is fixed by σ and hence $\alpha^3 \in \mathbb{Q}(\zeta_3)$. Since this extension has degree two, a basis is $\{1, \zeta_3\}$, so we know there are $a, b \in \mathbb{Q}$ such that

$$\alpha^3 = a\zeta_3 + b.$$

In practice this is easy for a computer to do because it is just symbolic manipulation and reducing using the minimal polynomial. But, one must use $\alpha = \omega + \zeta_3(\omega^2 - 2) + \zeta_3^2(1 - \omega^2 - \omega)$; we get $a = 21$ and $b = 14$. Now define $\beta = \omega + \zeta_3^2\omega_2 + \zeta_3\omega_3$, then since the ω_i are real, $\beta = \overline{\alpha}$, but as $-1 = \omega + \omega_2 + \omega_3$ we get

$$3\omega = -1 + \alpha + \beta.$$

Now $\alpha^3 = 21\zeta_3 + 14$, so $\beta^3 = 21\zeta_3^2 + 14 = 21(-\zeta_3 - 1) + 14 = -21\zeta_3 - 7$. This means that

$$\omega = \frac{1}{3}\left(-1 + \big(21\zeta_3 + 14\big)^{1/3} + \big(-21\zeta_3 - 7\big)^{1/3}\right).$$

Finally, using the fact that

$$\zeta_3 = \cos(2\pi/3) + i\sin(2\pi/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

we get a complete solution by radicals. We will soon be able to do this in more generality when we study the theory of solvable extensions (Sec. 2.5) and cyclotomic extensions (Sec. 2.4).

2.3 Constructible Numbers

Now we come to an interesting use case of Galois theory which will let us solve a concrete geometric problem. We want to see what kinds of shapes and numbers can be constructed using a 'straightedge/ruler and compass'. A straightedge lets us draw the unique line segment between any two given distinct points, and a compass lets us draw a circle centered at one point and containing another.

Informally, a point $(x, y) \in \mathbb{R}^2$ will be constructible if, starting from $\{(0,0),(1,0)\}$ we can realize it using finitely many iterations of the following steps:

1. Using the straightedge to draw lines between any two previously constructed points (which we can make arbitrarily long).
2. Using the compass to draw a circle centered at one previously constructed point with another one lying on it.
3. Taking intersection points of lines or circles.

These intersections will be the constructible points. Let us rigorize this into a definition we can work with:

Definition 2.3.1 A point $(x, y) \in \mathbb{R}^2$ is 0-*constructible* if it is either $(0,0)$ or $(1,0)$. An n-constructible circle is a circle in $\mathbb{R}^2$ centered at an $(n-1)$-constructible point and containing an $(n-1)$-constructible point. An n-constructible line is a line (infinitely extending) in $\mathbb{R}^2$ which contains at least two $(n-1)$-constructible points.

A point is *n-constructible* if it is $(n-1)$-constructible or it is obtained as an intersection point of 2 n-constructible circles, an n-constructible line and circle, or 2 $(n-1)$-constructible lines. A point is *constructible by ruler and compass* if it is n-constructible for some $n \geq 0$. We denote the set of n-constructible points as $\mathcal{C}_n^2 \subset \mathbb{R}^2$, and the set of constructible points as $\mathcal{C}^2 = \bigcup_{n \geq 0} \mathcal{C}_n^2 \subset \mathbb{R}^2$.

Note that this recursive definition makes sense because an n-constructible point relies on n-constructible lines/circles, which only rely on $(n-1)$-constructible points, and we have defined the base case. This definition is obviously difficult to work with in this state, so half the work will not be Galois-theoretic but rather geometric.

We will call a number $x \in \mathbb{R}$ constructible if there is a $y \in \mathbb{R}$ such that $(x, y) \in \mathcal{C}^2$; the set of constructible numbers is $\mathcal{C} \subset \mathbb{R}$. We may draw the x-axis using the two starting points, and then construct the circle centered at $(0,0)$ and passing through $(1,0)$ or vice versa. This shows that -1 and 1 are 1-constructible, and like this by induction $\mathbb{Z} \times \{0\} \subset \mathcal{C}^2$.

Next observe that if two points are n-constructible, then their perpendicular bisector, two points along it, and thus their midpoints, are all $(n+2)$-constructible. Indeed, this is obvious from Fig. ??. Therefore, $(-1/2, 0), (1/2, 0) \in \mathcal{C}$, and so two distinct points along the y-axis are constructible. Now for any $(x, 0) \in \mathcal{C}^2$, $(0, x) \in \mathcal{C}^2$ because the circle centered at the origin containing $(x, 0)$ intersects the y-axis at $(0, x)$. Hence $\{0\} \times \mathbb{Z} \subset \mathcal{C}^2$. Of course, the converse is true too.

Proposition 2.3.2 *$(x, y) \in \mathcal{C}^2$ if and only if $(x, 0) \in \mathcal{C}^2$ and $(0, y) \in \mathcal{C}^2$. In particular, $\mathcal{C}^2 = \mathcal{C} \times \mathcal{C}$.*

Proof The last sentence follows from what we just said and the first part. If (x, y) is constructible (and nonzero), then the circle centered at (x, y) passing through the origin intersects the x-axis at both $(0, 0)$ and $(2x, 0)$, the latter of which is thus constructible. Hence the midpoint $(x, 0)$ is constructible. The same logic flipped works for $(0, y)$.

On the other hand, if $(x, 0)$ and $(0, y)$ are constructible, then taking the circle at $(x, 0)$ passing through $(0, 0)$ gives $(2x, 0)$, and then taking a perpendicular bisector of the segment between these let's us construct the vertical line at $(x, 0)$. Similarly we can construct the horizontal line at $(0, y)$, and then take their intersection. □

Because of this proposition, we can essentially forget about y coordinates and focus on $\mathcal{C}$. Observe that if $x \in \mathcal{C}$, then $-x \in \mathcal{C}$ by the circle centered at $(0, 0)$ and containing $(x, 0)$. The circle centered at $(x, 0)$ containing $(0, 0)$ shows that $2x \in \mathcal{C}$. By taking midpoints $x/2 \in \mathcal{C}$. Hence if $x, y \in \mathcal{C}$, then by taking midpoints $(x + y)/2 \in \mathcal{C}$, so $x + y \in \mathcal{C}$.

Unsurprisingly, we can also take products. It suffices to construct squares, because $xy = ((x + y)^2 - x^2 - y^2)/2$, for which it it suffices to square $x > 0$. We can further assume $x > 1$, because if not $x + 1 > 1$, whose square is $x^2 + 2x + 1$, and we can subtract off $2x + 1$. To do this, see Fig. ??: Extend the line from $(0, 0)$ to $(1, x)$, then its intersection point with the vertical at $(x, 0)$ has y coordinate x^2 by similarity of the two evident triangles.

We can use the same trick to divide for which it suffices to construct $1/x$. We can again assume x positive, and even $x > 1$, because if not just choose an integer $N > 1/x$, then $Nx > 1$, and $1/x = N \cdot 1/(Nx)$. To do it, draw the segment from $(x, 1)$ to $(0, 0)$, and the vertical above $(1, 0)$; these two intersect at $(1, 1/x)$ by similarity.

Theorem 2.3.3 *The constructible numbers $\mathcal{C}$ form a field, and $\mathbb{Q} \subset \mathcal{C} \subset \mathbb{R}$. In addition:*

1. *If $x \geq 0 \in \mathcal{C}$, then $\sqrt{x} \in \mathcal{C}$.*
2. *$\mathcal{C}$ is the smallest extension intermediate to $\mathbb{Q} \subset \mathbb{R}$ closed under positive square roots.*
3. *If $x \in \mathbb{R}$, then $x \in \mathcal{C}$ if and only if there is a series of extensions*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{R}$$

such that $[K_{i+1} : K_i] \leq 2$ for all i and $x \in K_n$.

Proof We just proved the first sentence as $\mathcal{C}$ is a field containing $\mathbb{Z}$. First let's prove (1): we may assume $x > 1$ by taking $1/x$ if necessary. Construct the midpoint $(M, 0)$ of x and 1, and then the circle centered at $(M, 0)$ and

containing (M, M). Construct the line $x = 1$; the equation for a circle shows that the y-coordinate of an intersection point satisfies

$$(1 - M)^2 + y^2 = M^2 \Rightarrow y^2 = 2M - 1 = x,$$

since $M = (1+x)/2$. Therefore one intersection point is $(1, \sqrt{x})$, which is what we wanted. For the remaining, we show that the following are equivalent for $\alpha \in \mathbb{R}$:

(i) $\alpha \in \mathcal{C}$.

(ii) There is a series of extensions $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset \mathbb{R}$ such that $[K_{i+1} : K_i] \leq 2$ and $x \in K_n$.

(iii) α is contained in every subfield of $\mathbb{R}$ which is closed under taking square roots of positive numbers.

These equivalences will prove (2) and (3) above. (1) trivially implies $(iii) \Rightarrow (i)$: Let $F \subset \mathbb{R}$ be closed under square roots, then we prove $(ii) \Rightarrow (iii)$ by induction on n. If $n = 0$ then $x \in \mathbb{Q} \subset F$ since the characteristic is zero, so assume $n \geq 1$ and that we have proven the $n - 1$ case. If $\alpha \in K_{n-1}$ then we are done, so assume $\alpha \notin K_{n-1}$, and therefore $K_{n-1}(\alpha) = K_n$ has degree 2 over K_{n-1}. Suppose $x^2 + ax + b$ is the minimal polynomial of α over K_{n-1}, so $a, b \in F$ by induction. By the quadratic formula, $2\alpha = -a \pm \sqrt{a^2 - 4b} \in \mathbb{R}$, and $\sqrt{a^2 - 4b} \in F$ by assumption, therefore $\alpha \in F$.

Finally, $(i) \Rightarrow (ii)$ remains. (i) implies that $(\alpha, 0) \in \mathcal{C}^2$, and thus $\alpha \in \mathcal{C}^2_m$ for some $m \geq 0$. We show (ii) by induction on m. If $m = 0$, then $\alpha = 0$ or 1, so $\mathbb{Q} = K_0$ works. Otherwise, assume the $m \geq 1$ and that the $m - 1$ case is done. By definition, either $\alpha \in \mathcal{C}^2_{m-1}$, in which case we're done, or it is an intersection point of n-constructible circles or lines. In any of the cases, we will need 4 $(m - 1)$-constructible points to define these lines, i.e. 8 $(m - 1)$-constructible points of the form $(a, 0)$. This gives

$$\mathbb{Q} = L_0^{(i)} \subset \cdots \subset L_k^{(i)} \subset \mathbb{R}$$

with each step at most degree two for $i = 1, \ldots, 8$. But given two extension towers like this we can always make a bigger one containing both desired elements using the composite:

$$\mathbb{Q} \subset L_1^{(i)} \subset \cdots \subset L_k^{(i)} \subset L_k^{(i)} L_1^{(j)} \subset \cdots \subset L_k^{(i)} L_{k'}^{(j)}$$

We know from our results on composites that each step has at most degree two. Therefore, we may assume that we have already constructed a field $K_n \subset \mathbb{R}$ with a degree two tower over $\mathbb{Q}$ that contains the coordinates for any of the four points needed to define α.

If $(\alpha, 0)$ is at the intersection of two lines, the equation is of the form $y = ax + b = cx + d$ with $a, b, c, d \in K_n$, so $(d - b)/(a - c) \in K_n$, and the extension tower we already have works. If one of the defining shapes is a circle, its

equation will be of the form

$$(y - a_1)^2 + (x - b_1)^2 = r^2,$$

where $a_1, b_1, r^2 \in K_n$ because the center has coordinates in K_n, and the square of the distance from (a_1, b_1) to the second point is in K_n. If $(\alpha, 0)$ is at the intersection point it, in particular, must satisfy this equation. In other words,

$$a_1^2 + (\alpha - b_1)^2 = r^2$$

is a monic degree 2 relation for α over K_n, so $K_n(\alpha)/K_n$ has degree 2 and is contained in $\mathbb{R}$. This completes the induction step. □

This translates constructibility into a completely algebraic notion, so luckily we won't need to do any more geometry. We will use Galois theory to classify exactly when numbers are constructible. We will also consider the notion of constructibility of complex numbers, and that will turn out to be the most practical. The following lemma will do most of the work.

Lemma 2.3.4 *Let K be a field with* $\operatorname{char} K \neq 2$ *and let $\alpha \in \overline{K}$. The following are equivalent:*

(i) There is a sequence of extensions

$$K = K_0 \subset \cdots \subset K_n$$

such that $[K_{i+1} : K_i] \leq 2$ for all i and $\alpha \in K_n$.

(ii) There is a sequence of extensions

$$K = K_0 \subset \cdots \subset K_n$$

such that $[K_{i+1} : K_i] \leq 2$ for all i, and there are $\alpha_i \in K_i$ such that $K_i = K_{i-1}(\alpha_i)$ and $\alpha_i^2 \in K_{i-1}$, and $\alpha \in K_n$.

(iii) α is contained in normal extension of degree a power of 2.

Proof $(i) \Rightarrow (ii)$ More generally, we may prove that, in $\operatorname{char} K \neq 2$, if L/K has degree 2 there is a primitive element α such that $\alpha^2 \in K$. Indeed, choose any $\beta \in K$ and let x^2+ax+b be its minimal polynomial. Then $(2\beta+a)^2 = a^2-4b$ by the quadratic equation, so $(2\beta+a)^2 \in K$, and $\alpha = 2\beta+a$ generates $K(\beta) = L$.

$(ii) \Rightarrow (iii)$ Suppose we have such extensions $\{K_i\}$. We construct a sequence $\{L_i\}$ of extensions inductively such that (1) $L_i \supset K_i$, (2) L_i/L_{i-1} has degree a power of 2, and (3) L_i/K is normal. This suffices because, taking $i = n$, we see the degree L_n/K is a power of 2 by induction, it is normal, and $\alpha \in L_n$.

To do this, set $L_0 = K_0$ and now assume L_{i-1} has been defined. Let $\{\alpha_i^{(1)}, \ldots, \alpha_i^{(k)}\}$ be the set of conjugates of $\alpha_i = \alpha_i^{(1)}$ over K, and then set $L_i = L_{i-1}(\alpha_i^{(1)}, \ldots, \alpha_i^{(k)})$. Then L_i clearly contains K_i, and it is the composite of L_{i-1} and $K(\alpha_i^{(1)}, \ldots, \alpha_i^{(k)})$ which are normal, so L_i/K is normal.

Finally, since these are conjugate over K there is for any j an automorphism $\sigma\colon \overline{K} \to \overline{K}$ such that $\sigma(\alpha_i) = \alpha_i^{(j)}$. Since L_{i-1} is normal over K, σ preserves it; so since $\alpha_i^2 \in L_{i-1}$, $\sigma(\alpha_i^2) = (\alpha_i^{(j)})^2 \in L_{i-1}$. Therefore in

$$L_{i-1} \subset L_{i-1}(\alpha_i) \subset L_{i-1}(\alpha_i, \ldots, \alpha + i^{(k)}) = L_i,$$

each step has either degree 1 or 2, so the overall degree is a power of 2.

$(iii) \Rightarrow (i)$ Let L/K be normal, degree a power of 2, and $\alpha \in L$. By Prop. 1.5.9, L/K can't be inseparable because $\operatorname{char} K \neq 2$ doesn't divide $[L : K]$. Thus L/K is separable, normal, and finite, so Galois; let $G = \operatorname{Gal}(L/K)$. This is a p-group, so by Lemma 2.2.3 it has an index 2 subgroup. Inductively, we can create a filtration

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

of subgroups where each step has index 2. By the Galois correspondence this gives a sequence

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

where $\alpha \in K_n$, and each step has degree 2. □

One observes that almost all of this proof works if we replace 2 by some $p > 0$. In fact, it is the most trivial step, namely $(i) \Rightarrow (ii)$, which doesn't work in general. But, we will see in Sec. 2.5 that it works if we assume K contains pth roots of unity. We can now prove our fundamental result on constructible numbers.

Theorem 2.3.5 *The following are equivalent for a real number α.*

(i) $\alpha \in \mathcal{C}$.

(ii) *There is a series of real extensions $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset \mathbb{R}$ where $[K_{i+1}, K_i] \leq 2$ for all i, and $\alpha \in K_n$.*

(iii) *α is contained in a normal extension of degree a power of 2.*

(iv) *The splitting field of α has degree a power of 2 over $\mathbb{Q}$.*

The following are equivalent for real numbers α, β.

(i) *α and β are constructible.*

(ii) $(\alpha, \beta) \in \mathcal{C}^2$.

(iii) *There is a series of extensions $\mathbb{Q} = K_0 \subset \cdots \subset K_n$ where $[K_{i+1}, K_i] \leq 2$ for all i, and $\alpha + i\beta \in K_n$.*

(iv) *$\alpha + i\beta$ is contained in a normal extension of degree a power of 2.*

(v) *The splitting field of $\alpha + i\beta$ has degree a power of 2 over $\mathbb{Q}$.*

Proof We already know most of the equivalences. For part (1), we have seen $(i) \Leftrightarrow (ii)$, and $(iii) \Leftrightarrow (iv)$ is trivial because any normal extension containing α must contain the splitting field, and any subextension must have degree a

power of 2. The same proof shows $(iv) \Leftrightarrow (v)$ in part (2), and we have already seen $(i) \Leftrightarrow (ii)$. Moreover, the previous lemma gives $(iii) \Leftrightarrow (iv)$ in part (2).

First, let us show $(ii) \Leftrightarrow (iii)$ in part (1). The previous lemma immediately shows that $(ii) \Rightarrow (iii)$, so assume (iii). The lemma then gives a chain of fields $\mathbb{Q} = K_0 \subset \cdots \subset K_n$ where $\alpha \in K_n$, but each extension may not be contained in $\mathbb{R}$. Instead, consider the tower

$$\mathbb{Q} = K_0 \cap \mathbb{R} \subset K_1 \cap \mathbb{R} \subset \cdots \subset K_n \cap \mathbb{R}.$$

We know $\alpha \in K_n \cap \mathbb{R}$, so it suffices to show each extension has degree ≤ 2. Well, definitely $K_{i+1} \cap \mathbb{R}/K_i \cap \mathbb{R}$ is finite because

$$K_{i+1} \supset K_{i+1} \cap \mathbb{R} \supset \mathbb{Q}$$

is a tower of finite extensions. It is also separable, so let β be a primitive element of $K_{i+1} \cap \mathbb{R}$ over $K_i \cap \mathbb{R}$. Then assuming $\beta \notin K_i$, it satisfies a degree 2 polynomial $f \in K_i[x]$, but a polynomial cannot have one nonreal root so the other root is real. Therefore $f \in \mathbb{R}[x]$, so $f \in (K_i \cap \mathbb{R})[x]$ is a degree two polynomial, so the degree of the extension is less than 2. This finishes part (1).

To complete (2), first we do $(iv) \Rightarrow (i)$. Let $L/\mathbb{Q}$ be a normal extension of degree a power of 2 containing $\alpha + i\beta$. The automorphism $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ that is complex conjugation must preserve L, so $\alpha - i\beta \in L$, and thus $\alpha, \beta \in L$ by adding/subtracting and dividing by i. Hence α and β are real numbers contained in a normal extension of $\mathbb{Q}$ of degree a power of 2, so by part (1) they are constructible.

Finally, assume α and β are constructible. Let $\mathbb{Q} = K_0 \subset \cdots \subset K_n$ and $\mathbb{Q} = L_0 \subset \cdots L_m$ be the corresponding real sequences from part (1) where $\alpha \in K_n$ and $\beta \in L_m$. Consider the tower

$$\mathbb{Q} = K_0 \subset \cdots K_n = K_n L_0 \subset K_n L_1 \subset \cdots K_n L_m \subset K_n L_m(i).$$

Each step at the beginning is degree 2, and then

$$[L_{i+1}K_n : L_i K_n] \leq [L_{i+1} : K_i] \leq 2,$$

because $L_{i+1}K_n = (L_i K_n)L_{i+1}$. Finally, the last extension obviously has degree $\leq$ two because i is a root of $x^2 + 1$. □

This gives us a practically computable to check whether numbers and shapes are constructible or not. This is useful in some cases, as we will now see in some examples.

Example 2.3.6 (squaring the circle) An old question was whether one could, with a ruler and compass as described, construct a square with the area of of a unit circle. In fact one cannot: the sidelengths would have to be $\sqrt{\pi}$, and constructing two adjacent endpoints $\vec{v}, \vec{w} \in \mathbb{R}^2$ would mean we can construct

$\vec{v} - \vec{w} = (a, b)$, and hence $\pi = a^2 + b^2$. This is impossible since π is transcendental; a proof of this fact, which is elementary but somewhat annoying, will be left to an appendix.

Let us see for which n a regular n-gon in the plane can be constructed by ruler and compass. We claim this can be done if and only if the complex number $e^{2\pi i/n}$ is constructible in the sense of the previous theorem (either its real and complex parts are constructible, or identifying $\mathbb{C} = \mathbb{R}^2$ it is constructible). Indeed, if $\zeta_n = e^{2\pi i/n}$ is constructible, then ζ_n^k is constructible for $k = 0, \ldots, n-1$, which give the n vertices of a regular n-gon. On the other hand, if one can be constructed in the plane with center $z_0 \in \mathbb{C}$ and w_1, w_2 adjacent edges, $(w_2 - z_0)/(w_1 - z_0)$ (or the other way around) is equal to $|w_1|\,\zeta_n$.

Proposition 2.3.7 *Let $p \geq 3$ be a prime. A regular p-gon in $\mathbb{R}^2$ is constructible by ruler and compass if and only if $p = 2^k + 1$ for some $k \geq 1$ (i.e. p is a Fermat prime).*

Proof Recall that $\mathbb{Q}(\zeta_p)$ is the splitting field of ζ_p and is a degree $p-1$ extension of $\mathbb{Q}$. Hence we are done since ζ_p is constructible if and only if its splitting field has degree a power of 2. □

Once we study cyclotomic extensions we can extend this result to all $n \geq 3$, not just primes. The only known primes of this form are 3, 5, 17, 257, 65537, and it is conjectured that there are no more.[1]

2.4 Cyclotomic Extensions

The goal in understanding cyclotomic extensions, is to figure out the nth roots of unity in a field, and their minimal polynomials. So, let K be a field and consider the polynomial $f(x) = x^n - 1 \in K[x]$ for $n \geq 2$. Its derivative is nx^{n-1}; if $\operatorname{char} K \mid n$, then this is zero, and otherwise n is invertible in K so $\frac{x}{n} f'(x) - f(x) = 1$, therefore f is coprime to its derivative. So, there are exactly n distinct nth roots of unity over K if and only if $\operatorname{char} K \nmid n$. This is the case we focus on in this section.

Let K be a field of characteristic coprime to $n \geq 2$, fix an algebraic closure $\overline{K}$, and let $R \subset K^\times$ be the set of n distinct roots of the equation $x^n - 1$. $1 \in K$ is such a root, and observe that the product of two roots is clearly a root; hence R is a subgroup of $K^\times$ of order n. By Lemma 1.3.10, R is a cyclic subgroup. Hence we may write

$$R = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$$

for some $\zeta \in R$ of order n. In particular, $K(\zeta)/K$ is Galois, so write $G = \operatorname{Gal}(K(\zeta)/K)$. We call any generator of R an *primitive* nth root of unity. The

[1] If $2^n + 1$ is prime, then in fact n is a power of 2. Indeed, if an odd prime p divides n, so $n = pk$, then $2^n + 1 = (2^k)^p + 1$ is divisible by $2^k + 1$.

number of primitive nth roots is just the order of $(\mathbb{Z}/nZ)^\times$, i.e. $\varphi(n)$, the number of positive integers less than n and coprime to n.

If we fix a primitive root ζ, then all of them are ζ^i for $(i,n)=1$. If $\sigma \in G$, then since $\sigma(\alpha^k) = \sigma(\alpha)^k$ and σ is injective, σ preserves the order of elements of R. Since it is an automorphism, σ permutes the set of primitive nth roots of unity. Defining

$$\Phi_{n,K}(x) \coloneqq \prod_{i,(i,n)=1} (x - \zeta^i)$$

for any primitive root ζ, this means $\Phi_{n,K}(x)$ is fixed by the Galois group G and hence $\Phi_{n,K}(x) \in K[x]$. In particular, $\Phi_{n,K}(\zeta) = 0$, so the minimal polynomial of ζ divides Φ, so $\deg \zeta \leq \varphi(n)$. If $\sigma \in G$, then $\sigma(\zeta) = \zeta^i$ for a unique $i \in (\mathbb{Z}/n\mathbb{Z})^\times$, and if $\sigma(\zeta) = \zeta^i$ and $\tau(\zeta) = \zeta^j$ then

$$(\sigma\tau)(\zeta) = \sigma(\zeta)^j = \zeta^{ij},$$

mapping ζ to $ij \pmod n$. It follows that any choice of primitive nth root gives an inclusion $G \leq (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore $\deg \zeta \mid \varphi(n)$. We have already seen that when $n = p$ is a prime and $K = \mathbb{Q}$, then $G = (\mathbb{Z}/pZ)^\times$ and $\Phi_{n,\mathbb{Q}}$ is the irreducible polynomial of ζ_n.

There is an interesting fact, namely that $\Phi_{n,K}(x)$ is actually the same for all K; more precisely, it is always in the image of the natural map $i\colon \mathbb{Z}[x] \to K[x]$ factoring through the prime field, and it is always the image of the same polynomial. To see this, when $K = \mathbb{Q}$ we observe that by definition $\Phi_n(x) \mid x^n - 1$ over $\mathbb{Q}$, and $\Phi_n(x)$ is monic, so $\Phi_{n,\mathbb{Q}}(x) \in \mathbb{Z}[x]$.

For general K we do it by induction. Obviously $\Phi_{1,K} = x - 1 = i(x-1)$. If we've proven it $< n$, observe that each number less than n appears exactly as a number coprime to a factor of n. Therefore, since $x^n - 1$ is a product of its linear factors we have

$$x^n - 1 = \prod_{i \mid n} \Phi_{i,K}(x), \tag{$*$}$$

so $x^n - 1 = i(g(x))\Phi_{n,K}(x)$ by the inductive hypothesis. Since we already know that $x^n - 1 = g(x)\Phi_{n,\mathbb{Q}}(x)$, it follows since $K[x]$ is a domain that $\Phi_{n,K}(x) = i(\Phi_{n,\mathbb{Q}}(x))$. So we have shown:

Proposition 2.4.1 *The nth cyclotomic polynomial $\Phi_{n,K}$ is equal to the image of $\Phi_n \coloneqq \Phi_{n,\mathbb{Q}} \in \mathbb{Z}[x]$ under the canonical map $\mathbb{Z}[x] \to K[x]$.*

These polynomials are important in understanding roots of unity over $\mathbb{Q}$, in which case we shall see that they are in fact all irreducible. We have already seen that

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1$$

for p a prime is irreducible. Notice that we can use this and formula $*$ to write down the polynomials inductively using polynomial division. It is easy to see that Φ_n is not always irreducible. Most trivially, by adjoining some root ζ_n we

get a splitting field of Φ_n. Note that this can happen even over a field of the form $\mathbb{F}_p$. For example, over $\mathbb{F}_{13}$, we have

$$\Phi_3(x) = (x-3)(x+4),$$

so the cube roots of unity already exist in this field even though it has no subfields. Moreover, there are fields K for which Φ_n doesn't split but it isn't irreducible. We have already mentioned that $K(\zeta_n)$ is always Galois with Galois group a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. If K is so that Φ_n is irreducible, then this is the full Galois group, so we have the -1 degree 2 automorphism, whose fixed field is $L = K(\zeta_n + \zeta_n^{-1})$. Then $K(\zeta)/L$ has order 2, so Φ_n is not irreducible over L but does not split.

For the rest of this section, we focus on the case of $\mathbb{Q}$, over which we show that $\Phi_n \in \mathbb{Z}[x]$ is irreducible for all n. Recall that over $\mathbb{Q}$, we view $\zeta_n = e^{2\pi i/n}$ in the complex numbers. Let us prove this in steps. If it's not irreducible, let $\Phi_n = fg$ where f is monic irreducible and g is arbitrary, hence g is monic and $f, g \in \mathbb{Z}[x]$. Since Φ_n is separable, f is monic irreducible, and our assumption means $\deg g \geq 1$, there are $\zeta^i \neq \zeta^j$ primitive such that $f(\zeta^i) = 0$ and $g(\zeta^j) = 0$. Then $f(\zeta^j) \neq 0$ and $g(\zeta^i) \neq 0$.

Claim *There is a primitive nth root ζ_0 and a prime $p \leq n$ with $p \nmid n$ and $f(\zeta_0) = 0$ and $g(\zeta_0^p) = 0$.*

Proof Since $i, j \in (\mathbb{Z}/nZ)^\times$, write $r = ji^{-1} \pmod n$ so that $(\zeta^i)^r = \zeta^j$. Now write $r = \prod_{k=1}^m p_k$ as a product of primes so that each $p_k \nmid n$ since $(r, n) = 1$. Of the numbers $\{(\zeta^i)^{p_1 \cdots p_k} : k = 1, \ldots, m\}$, take k smallest so that

$$g((\zeta^i)^{p_1 \cdots p_k}) = 0,$$

which exists because m is such a k. If $k = 1$, then take $\zeta_0 = \zeta^i$ and $p = p_1$; otherwise, $\zeta_0 \coloneqq (\zeta^i)^{p_1 \cdots p_{k-1}}$ is still primitive, and is not a root of g so it must be a root of f, and $\zeta_0^{p_k}$ is a root of g. □

With this intermediate claim, the rest of the proof of the theorem is easy.

Theorem 2.4.2 *Let $n \geq 1$. The nth cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. In particular, the monomorphism*

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \qquad \sigma \mapsto i \text{ s.t. } \sigma(\zeta_n) = \zeta_n^i.$$

is an isomorphism.

Proof As before, it suffices to show the first part, and assuming the contrary we may factor $\Phi_n = fg$ where f is monic irreducible and $f, g \in \mathbb{Z}[x]$. By the previous claim, there is a primitive nth root of unity ζ_0 that is a root of f and $p \nmid n$ such that ζ_0^p is a root of g. So $f(x) = \mathrm{Irr}(\zeta_0, \mathbb{Q}, x)$, and since $g(x^p)$ has root ζ_0 we know $f(x) \mid g(x^p)$. Thus there is a $q \in \mathbb{Q}[x]$ such that $f(x)q(x) = g(x^p)$, so by monicity $q \in \mathbb{Z}[x]$.

Now let us reduce mod p: if $\overline{g} \in \mathbb{F}_p[x]$ is the image of g, then since the Frobenius fixes $\mathbb{F}_p$ we see

$$\overline{g}(x)^p = \left(\sum_i a_i x^i\right)^p = \sum_i a_i (x^p)^i = \overline{g}(x^p).$$

So $\overline{f}(x) \mid \overline{g}(x)^p$ over $\mathbb{F}_p$; if $w(x) \in \mathbb{F}_p[x]$ is any irreducible factor of $\overline{f}(x)$, then this means $w(x) \mid \overline{g}(x)$, so $w(x)^2 \mid \overline{f}\overline{g}(x) \mid x^n - 1$ in $\mathbb{F}_p[x]$. This implies that $\mathbb{F}_p[x]$ is not separable, which is a contradiction since $p \nmid n$ and we already showed that when $\operatorname{char} K \nmid n$, $x^n - 1$ is separable. □

The extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ over $\mathbb{Q}$ are called the cyclotomic extensions, and we will use this result many times throughout our study of Galois theory. Our first corollary relates to constructible numbers as discussed in the previous section.

Corollary 2.4.3 *Let $n \geq 3$. A regular n-gon is constructible by ruler and compass if and only if $\varphi(n)$ is a power of 2.*

Proof This is clear from the discussion in the previous section, in particular a regular n-gon is constructible iff ζ_n is constructible, if and only if the splitting field of ζ_n (which is $\mathbb{Q}(\zeta_n)$) has degree a power of 2 over $\mathbb{Q}$. □

On a very related note, the cyclotomic extensions help us understand the numbers $\cos(2\pi/n) \in \mathbb{R}$; we will write $\omega_n = 2\cos(2\pi/n)$, so that $\omega = \zeta_n + \zeta_n^{-1}$. Clearly this is the orbit of the element $-1 \in (\mathbb{Z}/n\mathbb{Z})^\times$, so $\mathbb{Q}(\omega) \subset \mathbb{Q}(\zeta_n)^{\{1,-1\}}$. On the other hand, if $\sigma(\zeta) = \zeta^j$ for some σ in the Galois group, then σ fixing ω would imply that

$$\zeta_n + \zeta_n^{-1} = \zeta_n^j + \zeta_n^{-j} = 2\cos(2\pi j/n).$$

Since $0 \leq j \leq n$, the only j for which $\cos(2\pi j/n) = \cos(2\pi/n)$ is $j = 1, n-1$. This implies that the fixed field of $\{\pm 1\} \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is exactly $\mathbb{Q}(\omega_n)$, and so it has degree $\varphi(n)/2$ over $\mathbb{Q}$. First of all, this means that $\cos(2\pi i/n)$ is rational only when $n \leq 3$. We also have the following obvious consequence of our previous work on constructible numbers (Thm. 2.3.3).

Corollary 2.4.4 *For $n \geq 3$, the real number $\cos(2\pi/n)$ is expressible from the rationals in terms of standard operations and square roots if and only if $\varphi(n)$ is a power of 2.*

Example 2.4.5 Everyone knows that $\cos(2\pi/3) = 1/2$. Let's write down $\omega = \omega_5 = 2\cos(2\pi/5)$ using square roots. $\varphi(5)/2 = 2$, so we know ω satisfies a degree 2 polynomial. Observing that $\zeta^{-2}\Phi_5(\zeta) = 0$, note that

$$\zeta^2 + \zeta^{-2} + \omega + 1 = 0,$$

and $\omega^2 = \zeta^2 + 2 + \zeta^{-2}$, so $\omega^2 - 2 + \omega + 1 = \omega^2 + \omega - 1 = 0$. The positive solution is $\omega = (\sqrt{5} - 1)/2$, so

$$\cos(2\pi/5) = \frac{\sqrt{5} - 1}{4}.$$

As we noted previously, the next prime we can do this for is $p = 17$, and it is visibly nontrivial that we can write $\cos(2\pi/17)$ using only square roots.

2.5 Solvable and Artin-Schreier Extensions

This section will be about the relationship between solvability of the Galois group of a polynomial and its solutions. We will see, in characteristic 0, that roughly a polynomial is solvable using nth roots (for any n) exactly when the Galois group is solvable. We will in fact be able to get more specific results.

Let us begin with the easy direction: necessity. Let K be a field of characteristic 0, and let $\alpha \in \overline{K}$ be some algebraic element. We will say that α is *expressible by radicals* over K if there is a chain of fields

$$K = K_0 \subset \cdots \subset K_n$$

such that $\alpha \in K_n$, and there are $\alpha_i \in K_i$ and positive integers k_i with $K_i = K_{i-1}(\alpha_i)$ and $\alpha_i^{k_i} \in K_{i-1}$. So, over $\mathbb{Q}$ this clearly corresponds to being able to write α in terms of nth roots for various n. The following definition is central to this section.

Definition 2.5.1 Let L/K be a Galois extension. L/K is *solvable* if $\mathrm{Gal}(L/K)$ is a solvable group.

Recall from group theory that all subgroups and quotients of a solvable group are solvable, and if $N \leq G$ is a normal subgroup such that N and G/N are solvable, then G is solvable. Here is the basic consequence:

Proposition 2.5.2 *Let L/K be a Galois extension.*

1. *For any F such that $K \subset F \subset L$, L/F is solvable.*
2. *For any normal intermediate extension F/K such that $K \subset F \subset L$, F/K is solvable.*

We write L_α for the the field generated by the conjugates of α, or $K(\alpha)^{\mathrm{nor}}$ the normal closure, or the splitting field of $\mathrm{Irr}(\alpha, K, x) \in K[x]$. L_α/K is Galois, so let $G = \mathrm{Gal}(L_\alpha/K)$ be the Galois group. This is a finite Galois extension.

References

[STK] The Stacks project authors, *The stacks project*, https://stacks.math.columbia.edu, 2024.