Exercises in Galois Theory

Arpon Basu

April 22, 2024

1 Basic Algebra

Exercise 1.1. *Show that* $p(X) := X^3 - nX + 2$ *is irreducible over* $\mathbb{Q}$ *for* $n \neq -1, 3, 5$.

Proof. Since p is a primitive polynomial, by Gauss's lemma it is enough to prove that p is irreducible on $\mathbb{Z}[X]$ to show it is irreducible on $\mathbb{Q}[X]$.
If p is irreducible, it must either factor into a quadratic and a linear polynomial, or three linear polynomials. In either case, it must have a rational root.
By the rational root theorem, if a/b is a root of p, then $a \mid 2$, and $b \mid 1$. Consequently, $\pm 1, \pm 2$ can be the only rational roots of p. Substituting these 4 values into p yield $n = -1, 3, 5$, and thus if $n \neq -1, 3, 5$, then p is irreducible over $\mathbb{Q}$. □

Exercise 1.2. *Let G be a p-group, i.e. $|G| = p^n$ for some prime p. Then G admits a* normal series decomposition, *i.e.*

$$G = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = 1$$

where G_{i+1} is a normal subgroup of G_i, and $|G_i| = p^{n-i}$.

Proof. We build inductively. Thus, suppose G_k is a normal subgroup of G of order $p^k, k < n$. It is clear that G_0 exists. Now, G/G_k is a p-group, and thus by standard class theory arguments, $Z(G/G_k) \neq 1$. Thus, by Cauchy's theorem, there exists $v \in Z(G/G_k)$ such that $\mathrm{ord}(v) = p$. Consider the subgroup $H := \langle v \rangle \subseteq Z(G/G_k)$. Since H is a subgroup of $Z(G/G_k)$, H is a normal subgroup of G/G_k. Now, by the third isomorphism theorem, if K is a group and N is a normal subgroup of K, then the normal subgroups of K and K/N correspond through the projection epimorphism $\pi : K \mapsto K/N$ (i.e. all the normal subgroups of K/N may be obtained by projecting the normal subgroups of K).
Thus, the pullback of $H \subseteq G/G_k$ into G is a normal subgroup of G. But the pullback of H into G has size $= |H| \cdot |G_k| = p \cdot p^k = p^{k+1}$, as desired. □

2 Field Extensions

Exercise 2.1. *Calculate the minimal polynomial of $\sqrt[4]{-2}$ over $\mathbb{Q}(\sqrt[4]{2})$.*

Proof. Note that the minimal polynomial of $\sqrt[4]{-2}$ over $\mathbb{Q}$ is $X^4 + 2$. Consequently, it's minimal polynomial over $\mathbb{Q}(\sqrt[4]{2})$ must be a divisor of $X^4 + 2$. Now, consider the factorization of $X^4 + 2$ over $\mathbb{Q}(\sqrt[4]{2})$:

$$X^4 + 2 = (X^2 - 2^{3/4}X + \sqrt{2})(X^2 + 2^{3/4}X + \sqrt{2})$$

$\sqrt[4]{-2}$ satisfies the first polynomial. Since $\sqrt[4]{-2} \notin \mathbb{Q}(\sqrt[4]{2})$, the minimal polynomial is of degree ≥ 2, and consequently, $X^2 - 2^{3/4}X + \sqrt{2}$ is the desired polynomial. □

Exercise 2.2. *Show that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.*

Proof. It is enough to show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Indeed, $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, and thus $\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, and consequently, $5-2\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. However, $5-2\sqrt{6} = (\sqrt{3}-\sqrt{2})^2 = \frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}+\sqrt{2}}$, and consequently $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, which yields that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, as desired.
If we substitute $X = \sqrt{2}+\sqrt{3}$, then $X^2 = 5+2\sqrt{6}$, and thus $(X^2-5)^2 = 24 \implies X^4 - 10X^2 + 1 = 0$. Now,

$$X^4 - 10X^2 + 1 = (X - (\sqrt{2}+\sqrt{3}))(X - (-\sqrt{2}+\sqrt{3}))(X - (\sqrt{2}-\sqrt{3}))(X - (-\sqrt{2}-\sqrt{3}))$$

Clearly, no linear polynomial in $\mathbb{Q}[X]$ divides $X^4 - 10X^2 + 1$, so if at all $X^4 - 10X^2 + 1$ factorizes over $\mathbb{Q}$, it must split into 2 quadratic polynomials. However, by checking all 6 combinations of two numbers $\alpha, \beta \in \{\pm\sqrt{2} \pm \sqrt{3}\}$, we see that either $\alpha + \beta \notin \mathbb{Q}$, or $\alpha\beta \notin \mathbb{Q}$.
Consequently, $X^4 - 10X^2 + 1$ is irreducible over $\mathbb{Q}$, and thus is the minimal polynomial of $\sqrt{2}+\sqrt{3}$. □

Aliter. Note that $[\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}(\sqrt{2})]$. Since $\sqrt{3}$ satisfies $X^2 - 3$, we have $[\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$, $[\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \neq 1$. Thus $[\mathbb{Q}(\sqrt{3},\sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, as desired. □

Exercise 2.3. *Prove that $X^n - 2$ is irreducible over $\mathbb{Q}$ for $n \geq 2$. Conclude that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Deduce that $\overline{\mathbb{Q}}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ aren't finite extensions.*

Proof. The irreducibility follows from Eisenstein's criterion. □

Exercise 2.4. *Let F be a finite field. Prove that $|F| = p^n$ for some prime p.*

Proof. Consider the ring homomorphism $\phi : \mathbb{Z} \mapsto F$, i.e. $\phi(1) = 1$. Now, $\ker(\phi) \subseteq \mathbb{Z}$ can't be (0), because otherwise ϕ would be injective, which isn't possible, since $\mathbb{Z}$ is infinite, and F is finite. Thus $\ker(\phi) = (p)$ (since the only non-trivial ideals of $\mathbb{Z}$ are (p) for primes p).
Then, by the first isomorphism theorem, we have an injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. Now, we claim that F is a $\mathbb{Z}/p\mathbb{Z}$-vector space: Indeed, $(F, +, 0)$ is an abelian group (since F is a field). Furthermore, for any $\overline{m} \in \mathbb{Z}/p\mathbb{Z}, x \in F$, define $\overline{m} \cdot x := mx$. Then it is easy to verify the axioms of a vector space (see this). □

Exercise 2.5. *Suppose α is such that $\deg_F(\alpha)$ is odd. Prove that $F(\alpha) = F(\alpha^2)$.*

Proof. Note that $F(\alpha) = F[\alpha]$. Furthermore, if $\deg_F(\alpha) = n$, then $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of $F(\alpha)$ (as a F-vector space). Since n is odd, $\{(2k) \bmod n : 0 \leq k \leq n-1\} = \{k : 0 \leq k \leq n-1\}$, and thus we're done. □

Exercise 2.6. *Let F be a field of characteristic $\neq 2$. Let $a, b \in F$, where b is not a perfect square in F. Prove that $\sqrt{a+\sqrt{b}}$ can be expressed as $\sqrt{m}+\sqrt{n}$, with $m, n \in F$, if and only if $a^2 - b$ is a square in F.*

Proof. If $\sqrt{a+\sqrt{b}} = \sqrt{m}+\sqrt{n}$, then $a+\sqrt{b} = m+n+2\sqrt{mn}$. Now, $\sqrt{mn} \notin F$, since otherwise we would have $\sqrt{b} \in F$. Now, the degree of $a+\sqrt{b}$ over F is 2 (it can't be 1, and $a+\sqrt{b}$ satisfies $X^2 - 2aX + (a^2-b) \in F[X]$). Similarly, $m+n+2\sqrt{mn}$ also has degree 2 over F. Since $a+\sqrt{b} = m+n+2\sqrt{mn}$, they must have the same minimal polynomial. Now, the other root of the minimal polynomial of $m+n+2\sqrt{mn}$ is $m+n-2\sqrt{mn}$, which must necessarily equal $a-\sqrt{b}$. Thus $a \pm \sqrt{b} = m+n \pm 2\sqrt{mn}$ (the signs correspond), and thus $\sqrt{b} = 2\sqrt{mn}$. Consequently we have $b = 4mn, a = m+n$.
Conversely, if $a^2 - b$ is a square, then by setting $m = (a+\sqrt{a^2-b})/2, n = (a-\sqrt{a^2-b})/2$, and doing some algebra we see $\sqrt{a+\sqrt{b}} = \sqrt{m}+\sqrt{n}$. □

Exercise 2.7. *Let $E/k, F/k$ be finite field extensions, with both E, F being contained in some larger field. Show that:*

1. $[EF : k] \leq [E : k][F : k]$.
2. *If* $[E : k], [F : k]$ *are relatively prime, then* $[EF : k] = [E : k][F : k]$.
3. *Does* $[EF : k]$ *divide the product* $[E : k][F : k]$*?*

Proof. The proofs are as follows:

1. Let $\{e_1, \ldots, e_n\}$ be a basis of E as a k-vector space, and let $\{f_1, \ldots, f_m\}$ be a basis of F as a k-vector space. Since $\{e_i\}_{i\in[n]}, \{f_j\}_{j\in[m]}$ are algebraic, $k(e_i, f_j)$ is a finite (and hence algebraic) extension of k, consequently, since $e_i f_j \in k(e_i, f_j)$, $e_i f_j$ is algebraic over k too. Thus, $k(\{e_i f_j\}_{i\in[n],j\in[m]})$ is a finite (and hence algebraic) extension of k. Now, note that every element of EF can be written as $\sum_r \varepsilon_r \phi_r / \sum_s \varepsilon'_s \phi'_s$, where the ε's belong to E, and the ϕ's belong to F. But $\varepsilon_r \phi_r, \varepsilon'_s \phi'_s$ can be written as a linear combination of $\{e_i f_j\}$, and thus $EF \subseteq k(\{e_i f_j\}_{i\in[n],j\in[m]})$. But note that $k(\{e_i f_j\}_{i\in[n],j\in[m]}) = k[\{e_i f_j\}_{i\in[n],j\in[m]}]$, and $\dim_k(k[\{e_i f_j\}_{i\in[n],j\in[m]}]) \leq mn = \dim_k(E)\dim_k(F)$, and thus $\dim_k(EF) \leq \dim_k(E)\dim_k(F)$.
2. Note that $[EF : k] = [EF : E][E : k]$, and thus $[E : k] \mid [EF : k]$. Similarly, $[F : k] \mid [EF : k]$. Since $[E : k], [F : k]$ are co-prime, $[E : k][F : k] \mid [EF : k]$. However, $[EF : k] \leq [E : k][F : k]$, and thus we're done.
3. No. Let $k = \mathbb{Q}, E = \mathbb{Q}(\sqrt[3]{2}), F = \mathbb{Q}(\sqrt[3]{2}\omega)$, where both E and F are embedded naturally in $\mathbb{C}$. Then $EF = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Now, the minimal polynomial of ω over $\mathbb{Q}$ is $X^2 + X + 1$. Thus $[EF : \mathbb{Q}] = [EF : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3[EF : \mathbb{Q}(\sqrt[3]{2})]$. Once again, $[EF : \mathbb{Q}(\sqrt[3]{2})] \leq 2$, and it can't be 1 since $\omega \notin \mathbb{Q}(\sqrt[3]{2})$. Thus $[EF : k] = 6$, while $[E : k] \cdot [F : k] = 9$, and 6 doesn't divide 9.

□

Exercise 2.8. *Let α, β be algebraic over F, such that the degrees of α, β are relatively co-prime. Let $g(X)$ be the minimal polynomial of β over F. Then $g(X)$ remains irreducible even in $F(\alpha)[X]$.*

Proof. Let $G = F(\alpha, \beta)$. Then $[F(\alpha) : F] \mid [G : F] \implies \deg_F(\alpha) \mid [G : F]$. Similarly, $\deg_F(\beta) \mid [G : F]$. Since the degrees are relatively co-prime, $\deg_F(\alpha) \cdot \deg_F(\beta) \mid [G : F]$. Since $[G : F] = [F(\alpha, \beta) : F(\alpha)] \cdot \deg_F(\alpha)$, we have $\deg_{F(\alpha)}(\beta) = [F(\alpha, \beta) : F(\alpha)] \geq \deg_F(\beta) \geq \deg_{F(\alpha)}(\beta)$. Thus $\deg_F(\beta) = \deg_{F(\alpha)}(\beta)$, and consequently, $g(X)$ is irreducible over $F(\alpha)[X]$ too. □

Exercise 2.9. *Show that there are no (non-identity) ring homomorphisms from $\mathbb{R}$ to itself. Conclude that $\mathbb{R}$ is not a finite extension of any proper subfield.*

Proof. Let $f : \mathbb{R} \mapsto \mathbb{R}$ be a ring homomorphism. By standard Cauchy equation analysis, $f|_{\mathbb{Q}} = \text{id}$.
Now, if $x \geq 0$, then $f(x) = f(\sqrt{x})^2 \geq 0$, thus, for any $a \leq b$, we have $f(a) \leq f(b)$, since $f(b - a) = f(b) - f(a)$. Now, let $x \in \mathbb{R}$ be any real number. Let $\{q_n\}_{n\in\mathbb{N}}$ be a sequence of rationals converging to x from below, and let $\{r_n\}_{n\in\mathbb{N}}$ be a sequence of rationals converging to x from above. We know that $f(x - q_n) \geq 0 \implies f(x) \geq q_n$. Similarly, $f(x) \leq r_n$. Thus $q_n \leq f(x) \leq r_n$, and applying the squeeze theorem yields $f(x) = x$. □

Exercise 2.10. *Produce a field k and an embedding $k \hookrightarrow k$ such that the extension k/k is infinite.*

Proof. Let F be an arbitrary field, and let $k = F(x_1, x_2, \ldots)$. Consider the embedding $k \hookrightarrow k$ induced by $x_i \mapsto x_{i+1}$ for all $i \in \mathbb{N}$. This extension is infinite, and in fact transcendental. □

Exercise 2.11. *Produce fields k_1, k_2, k_3, k_4 such that $k_1 \cong k_2, k_3 \cong k_4$, yet the extensions k_1/k_3 and k_2/k_4 aren't isomorphic.*

Proof. Take $k_1 = k_2 = k_3 = k(x)$, and $k_4 = k(x^2)$. k_3 is isomorphic to k_4, as is demonstrated by the embedding induced by $x \mapsto x^2$. However, k_1/k_3 is an extension of degree 1, while k_2/k_4 (where the embedding is the natural inclusion) is an extension of degree 2. □

Exercise 2.12. *Explain the following apparent paradox: $k(x) \cong k(x^2)$, yet $1 - x^2t^2$ is irreducible in $k(x^2)[t]$, while $1 - x^2t^2 = (1 - xt)(1 + xt)$ is not irreducible in $k(x)[t]$.*

Proof. $k(x)$ and $k(x^2)$ are isomorphic, but the natural embedding $k(x^2) \hookrightarrow k(x)$ is *not* an isomorphism; consequently, there is no paradox. Indeed, if one takes the image of the polynomial under the map induced by $x \mapsto x^2$, then one gets $1 - x^4t^2 = (1 - x^2t)(1 + x^2t)$, which is obviously not irreducible (and factorizes in the same way $1 - x^2t^2$ factorizes in $k(x)[t]$). □

Exercise 2.13. *Given any $n \in \mathbb{N}$, produce a field extension of degree n.*

Proof. The field extension $k(x^{1/n})/k(x)$, where the embedding is the natural inclusion, has degree n. Note that $k(x^{1/n}) := k(x)[t]/(t^n - x)$. □

Exercise 2.14. *Let k be an infinite field. If E/k is an algebraic extension, then the cardinality of E equals the cardinality of k. Conclude that $\mathbb{R}$ is not algebraic over $\mathbb{Q}$.*

Proof. By the embedding theorem, any algebraic E embeds in $\overline{k}$, so it suffices to show $|\overline{k}| = |k|$ (because we have $|k| \leq |E| \leq |\overline{k}|$). To do that, we shall construct a surjection $\phi : (k[X] - k) \times \mathbb{N} \mapsto \overline{k}$. For any $p \in k[X] - k$, let $\alpha_0, \ldots, \alpha_{n-1}$ (the ordering is arbitrary) be the roots of p in $\overline{k}$. Define $\phi(p, m) := \alpha_{m \bmod n}$. This is surjective, because $\overline{k}$ is algebraic over k, and thus for every $\alpha \in \overline{k}$, there is some $p \in k[X] - k$ such that $p(\alpha) = 0$. Thus $|(k[X] - k) \times \mathbb{N}| \geq |\overline{k}| \geq |k|$. But $|(k[X] - k) \times \mathbb{N}| = |k[X] - k| = |k|$, as desired. □

Remark. *A few remarks are in order:*

1. *Cardinal arithmetic: If A, B are infinite sets, then $|A \times B| = \max\{|A|, |B|\}$.*
2. *$|\overline{k}| = |k|$ for infinite fields k.*

Exercise 2.15. *If $[E : F] = p$ (p is a prime), then $E = F(\alpha)$ for* any *$\alpha \in E \setminus F$.*

Proof. $[F(\alpha) : F]$ must divide p. It can't be 1, since $\alpha \notin F$. Thus $[F(\alpha) : F] = p$, implying $E = F(\alpha)$. □

Exercise 2.16. *Let E/F be an extension. This extension is algebraic if and only if every subring of E containing F is a field.*

Proof. Suppose E/F is algebraic. Let $K \supseteq F$ be a subring, and let $\alpha \in K \setminus F$. Let $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be the minimal polynomial of α over F. Since $g(X)$ is irreducible, $a_0 \neq 0$. But note that

$$\alpha^{-1} = (-a_0)^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-1} + \cdots + a_1) \in F[\alpha] \subseteq K$$

Thus, if $\alpha \in K$, then $\alpha^{-1} \in K$, and thus, K is a field.
Conversely, suppose E/F is not algebraic. Then we have some $t \in E$ which is transcendental over F. Then note that $F[t]$ is a ring containing F, but $F[t]$ is not a field since $t^{-1} \notin F[t]$. □

Exercise 2.17. *Let k be a field, and let $\alpha = p(X)/q(X)$ be an element of $E := k(X)$, where $p(X), q(X) \in k[X] - k$, $p(X), q(X)$ are co-prime. Show that $E/k(\alpha)$ is a finite extension, with $[E : k(\alpha)] = \max(\deg(p), \deg(q))$.*

Proof. Consider the polynomial $f(T) := p(T) - \alpha q(T) \in k(\alpha)[T]$. Note that $f(X) = 0$, and thus $X \in E$ is algebraic over $k(\alpha)$, with degree at most $\deg(f) = \max(\deg(p), \deg(q))$. Since E is generated by X over k (and hence $k(\alpha)$), $[E : k(\alpha)] \leq \deg(f)$. Consequently, if we can show that f is irreducible in $k(\alpha)[T]$, then f would be the minimal polynomial of X, and we would have $[E : k(\alpha)] = \deg(f) = \max(\deg(p), \deg(q))$.
Now, by Gauss's lemma, to show that f is irreducible in $k(\alpha)[T]$, it is enough to show that it is irreducible in $k[\alpha][T] \cong k[T][\alpha]$. But note that α is a prime element in $k[T][\alpha]$, and consequently, by Eisenstein's criterion applied on f with the prime α, we get that it is irreducible. □

Exercise 2.18. *Let $E = F(x)$, where x is transcendental over F. Let K be a subfield of E containing F such that $K \neq F$. Then x is algebraic over K.*

Proof. Direct corollary of Exercise 2.17. □

Exercise 2.19. *Prove that every element is a sum of two squares in $\mathbb{F}_p$.*

Proof. Note that $\#\{x^2 : x \in \mathbb{F}_p\} = (p+1)/2$. Indeed, the group $(\mathbb{F}_p^\times, \cdot, 1)$ has $(p-1)/2$ squares, since it is cyclic (and hence exactly the even powers of the generator are squares), and 0 is also a square. Thus, given any $x \in \mathbb{F}_p$, consider the set $\{x - y^2 : y \in \mathbb{F}_p\}$. This set also has size $(p+1)/2$. Consequently, by the pigeonhole principle, the sets $\{x - y^2 : y \in \mathbb{F}_p\}$ and $\{z^2 : z \in \mathbb{F}_p\}$ intersect, i.e. $x - y_0^2 = z_0^2$ for some $y_0, z_0 \in \mathbb{F}_p$. But that means $x = y_0^2 + z_0^2$, as desired. □

Exercise 2.20. *A field is called formally real if -1 is not a sum of squares in it. Let k be a formally real field. Let K/k be an odd extension. Prove that K is formally real.*

Proof. Note that $\mathrm{char}(k) = 0$, because positive characteristics contain $\mathbb{F}_p$, and -1 is a sum of squares in $\mathbb{F}_p$. Thus K/k is a finite separable extension, and hence simple. Thus, let $K = k(\alpha)$. We induct on $\deg_k(\alpha)$. The base case is trivial.
Assume for the sake of contradiction that -1 is a sum of squares in K. Then

$$-1 = \sum_i p_i(\alpha)^2 \implies 1 + \sum_i p_i(\alpha)^2 = 0$$

where p_i's are polynomials such that $\deg(p_i) < \deg_k(\alpha)$. Define

$$p(X) := 1 + \sum_i p_i(X)^2$$

Denote the minimal polynomial of α over k as $f(X)$. Since α is a root of p, $f(X) \mid p(X)$. Denote $q(X) := p(X)/f(X)$. Now, note that $\deg(p) \leq 2(\deg_k(\alpha) - 1)$, and thus $\deg(q) \leq \deg_k(\alpha) - 2$. We also claim that the degree of p is even: Indeed, let the highest degree of any of the p_i's be m, and suppose $p_{i_1}, \ldots, p_{i_r}$ have degree m. Then the coefficient of X^{2m} is $c_{i_1}^2 + \cdots + c_{i_r}^2$, where c_{i_*} is the coefficient of X^m in p_{i_*}. However, since k is formally real, $c_{i_1}^2 + \cdots + c_{i_r}^2 \neq 0$ since $c_{i_*} \neq 0$.
Thus, $\deg(q)$ is an odd number which is at most $\deg_k(\alpha) - 2$. Consequently, factorizing q over k, we get that q must have an irreducible divisor of odd degree. Let β be a root of that divisor. Then $k(\beta)$ is formally real by the induction hypothesis, and β is a root of p. But then p expresses -1 as a sum of squares in $k(\beta)$, which is a contradiction. □

Remark: If $c_1^2 + \cdots + c_r^2 = 0$ for some $c_1, \ldots, c_r \in \mathbb{F} \setminus \{0\}$, then $(c_1/c_r)^2 + \cdots + (c_{r-1}/c_r)^2 = -1$.

3 Splitting Fields and Normal Extensions

Exercise 3.1. *Find the splitting fields of the following polynomials over* $\mathbb{Q}$*:* $X^4 - 2, X^4 + 2, X^4 + X^2 + 1, X^6 - 4, X^6 + X^3 + 1$.

Proof. The splitting fields are as follows:

1. $X^4 - 2$: $\mathbb{Q}(\sqrt[4]{2}, i)$. $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$: Indeed, adjoining $\sqrt[4]{2}$ to $\mathbb{Q}$ makes the degree 4. i doesn't belong to it, because i is non-real. Thus adjoining i doubles the degree.

2. $X^4 + 2$: $\mathbb{Q}(\sqrt[4]{2}, i)$.

3. $X^4 + X^2 + 1$: $\mathbb{Q}(i\sqrt{3})$, $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$.

4. $X^6 - 4$: $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$.

5. $X^6 + X^3 + 1$: $\mathbb{Q}(\zeta)$, where $\zeta = e^{2i\pi/9}$. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 9$.

□

Exercise 3.2. *Let* $\alpha = 5^{1/4}$*. Prove that:*

1. $\mathbb{Q}(i\alpha^2)$ *is normal over* $\mathbb{Q}$.

2. $\mathbb{Q}((1 + i)\alpha)$ *is normal over* $\mathbb{Q}(i\alpha^2)$.

3. $\mathbb{Q}((1 + i)\alpha)$ *is not normal over* $\mathbb{Q}$.

Proof. The proofs are as follows:

1. $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\sqrt{5})$ is the splitting field of $X^2 + 5$ over $\mathbb{Q}$.

2. Note that $\beta := (1 + i)\alpha = \sqrt{2} \cdot \sqrt[4]{-5}$. Thus $\beta^2 = 2i\sqrt{5} = 2i\alpha^2$, and thus $\mathbb{Q}(\beta)$ is the splitting field of $X^2 - 2i\alpha^2$ over $\mathbb{Q}(i\alpha^2)$.

3. $X^4 + 20$ has $(1 + i)\alpha$ as its root; however, $(1 - i)\alpha$ is also a root of $X^4 + 20$, yet $(1 - i)\alpha \notin \mathbb{Q}((1 + i)\alpha)$. Since $X^4 + 20$ is irreducible over $\mathbb{Q}$, $\mathbb{Q}((1 + i)\alpha)$ is not normal over $\mathbb{Q}$. To see how $(1 - i)\alpha \notin \mathbb{Q}((1 + i)\alpha)$, note that if $(1 - i)\alpha$ were in $\mathbb{Q}((1 + i)\alpha)$, then we would have $i, \alpha \in \mathbb{Q}((1 + i)\alpha)$, implying that $\mathbb{Q}(i, \alpha) \subseteq \mathbb{Q}((1 + i)\alpha)$. However, $[\mathbb{Q}(i, \alpha) : \mathbb{Q}] = 8$, while $[\mathbb{Q}((1 + i)\alpha) : \mathbb{Q}] = 4$.

□

Exercise 3.3. *Let* $f \in k[X]$ *be a polynomial of degree* d*. Let* L *be the splitting field of* f *over* k*. Then* $[L : k]$ *divides* $d!$.

Proof. We proceed by induction. $d = 1$ is easy to verify. So assume the statement is true for all $d < n$. Thus, assume $\deg(f) = n$. Now, we make cases:

1. Suppose f is irreducible over k. Let $\alpha \in L$ be a root of f. Then $f(X) = (X - \alpha)g(X)$, with $\deg(g) = n - 1$.

□

Exercise 3.4. *Find the splitting field of* $X^{p^n} - 1$ *over* $\mathbb{F}_p$.

Proof. Note that $(X-1)^{p^n} = X^{p^n} + (-1)^{p^n}$ over $\mathbb{F}_p$. If p is odd, $(-1)^{p^n} = -1$, in which case the splitting field is $\mathbb{F}_p$ itself. If $p = 2$, $(-1)^{p^n} = 1$, but we also have $-1 = 1$, so once again the splitting field is $\mathbb{F}_p = \mathbb{F}_2$. Thus the splitting field of $X^{p^n} - 1$ over $\mathbb{F}_p$ is $\mathbb{F}_p$, for all primes p, and all $n \geq 1$. □

Exercise 3.5. *Prove that for any prime p and any $n \geq 1$, we have a finite field of order p^n. Furthermore, all finite fields of order p^n are $\mathbb{F}_p$-isomorphic to each other.*

Proof. We shall prove that the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ is a finite field of order p^n.
Firstly, note that the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ must be finite since the splitting field can be obtained by adjoining the finitely many roots of $X^{p^n} - X$ (in $\overline{\mathbb{F}}_p$) to $\mathbb{F}_p$. Furthermore, by taking formal derivatives, we can see that all roots of $X^{p^n} - X$ are distinct.
Now, also note that the roots of $X^{p^n} - X$ form a field: Indeed, if α, β are roots, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Furthermore, $(\alpha\beta)^{p^n} = (\alpha^{p^n})(\beta^{p^n}) = \alpha\beta$, and if $\alpha \neq 0$, then $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. Finally, for any α, $(-\alpha)^{p^n} = (-1)^{p^n}\alpha$. If p is odd, then we obtain that $-\alpha$ is also a root of the polynomial $X^{p^n} - X$. If $p = 2$, then $-\alpha = \alpha$. Thus, for any α (which is a root of $X^{p^n} - X$), $-\alpha$ is also a root of $X^{p^n} - X$.
Thus the roots of $X^{p^n} - X$ form a field, and furthermore, this field contains $\mathbb{F}_p$. Thus, this field is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. It is clear that this field contains exactly p^n elements. Furthermore, all splitting fields are $\mathbb{F}_p$-isomorphic to each other. □

Exercise 3.6. *Prove that every finite extension of a finite field is normal.*

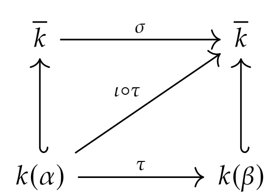
Proof. Let K/F be a field extension, with $|K| = q$. Then all elements of K satisfy the equation $X^q = X$, and thus K is the splitting field of F w.r.t the polynomial $X^q - X \in F[X]$. □

Exercise 3.7. *Prove that every algebraic extension of a finite field is normal.*

Proof. Let K/F be a field extension, where F is finite. Suppose $f \in F[X]$ has a root $\alpha \in K$. Since α is algebraic over F, $F(\alpha)/F$ is a finite extension and hence is a normal extension by the above exercise. Since f has a root in $F(\alpha)$, and since $F(\alpha)/F$ is normal, f splits completely over $F(\alpha)$, and hence K. Thus K/F is normal. □

Exercise 3.8. *Let K/k be a normal extension, and let $f(X) \in k[X]$ be irreducible over k, such that $f(X) = g(X)h(X)$ over K, where $g(X), h(X) \in K[X]$ are irreducible over K. Prove that there exists an k-automorphism σ of K such that $h = \sigma(g)$. State a counterexample to this assertion when K/k is not normal.*

Proof. Let F be the splitting field of f over k. Let α be a root of g in F, and let β be a root of h in F. Note that we can choose $\beta \neq \alpha$: Indeed, all roots of g and h are distinct, since if g and h had any common root, they would have a non-trivial gcd over F (and hence K), contradicting their irreducibility over K. Now, since α, β are both roots of the irreducible polynomial f over k, there exists an k-embedding $\tau : k(\alpha) \mapsto k(\beta)$ sending α to β. Now, consider the following diagram:



Let ι be the inclusion $k(\beta) \hookrightarrow \overline{k}$, and consider the map $k(\alpha) \xrightarrow{\iota\circ\tau} \overline{k}$. Since $\overline{k}$ is algebraic over $k(\alpha)$, and since $\overline{k}$ is algebraically closed, there exists a $k(\alpha)$-embedding σ from $\overline{k}$ to $\overline{k}$ such that $\sigma|_{k(\alpha)} = \iota \circ \tau$. Furthermore, $\sigma(K) = K$ since K is normal

over k, and thus $\sigma|_K$ is a k-automorphism. Consequently, $\sigma(g)$ is also a polynomial in $K[X]$, and furthermore, $\sigma(g)$ has $\sigma(\alpha) = \beta$ as a root. On the other hand, since σ is a k-automorphism and since $f \in k[X]$, $\sigma(f) = f$. Thus, $\sigma(g)$ is an irreducible (over K) factor of f having β as a root. Since h is the only irreducible factor of f having β as a root, $\sigma(g) = h$, as desired.
For a counterexample, consider $K = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, and let $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Then $f(X) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2} \cdot X + \sqrt[3]{4})$ over K. Both $(X - \sqrt[3]{2})$ and $(X^2 + \sqrt[3]{2} \cdot X + \sqrt[3]{4})$ are irreducible over K, but they are obviously not images of each other through some automorphism. □

4 Separable Extensions

Exercise 4.1. *Let* $\mathrm{char}(k) = p$. *Let* $f(X) \in k[X]$ *be an irreducible polynomial. Then* f *is not separable iff* $f(X) = g(X^p)$ *for some* $g(X) \in k[X]$. *Consequently, for any irreducible polynomial* $f(X) \in k[X]$, $f(X) = h(X^{p^n})$ *for some separable irreducible polynomial* $h(X) \in k[X]$ *and* $n \geq 0$.

Proof. If $f(X)$ is not separable, then $f(X)$ has repeated roots, and thus there is some $\alpha \in \overline{k}$ such that $f(\alpha) = f'(\alpha) = 0$. Now, if $f' \neq 0$, then f, f' have a non-trivial gcd over $\overline{k}$ and hence k (recall that gcd is a field invariant entity), which is not possible since f is irreducible. Thus $f' = 0$. But f' can be 0 only when the only non-zero coefficients of f are associated with powers of X^p, i.e. $f(X) = g(X^p)$.
Conversely, if $f(X) = g(X^p)$, then $f' = 0$, i.e. all roots of f are identical. Since f is irreducible over k, $\deg(f) > 1$, and consequently, f is not separable over k. □

Remark. *If* f *is an irreducible polynomial over* K *(where* K *is an arbitrary field) with* $f'(X) \neq 0$, *then all roots of* $f(X)$ *(over* $\overline{K}$*) are distinct. Indeed,* $X - \alpha$ *divides* $f(X), f'(X)$, *where* $\alpha \in \overline{K}$, *then* $f(X), f'(X)$ *would have a non-trivial gcd in* $\overline{K}$. *But the gcd of two polynomials is the same regardless of the field, so the gcd of* f, f' *would be non-trivial even over* K. *But* $f(X)$ *is irreducible over* K, *and can only have a non-trivial gcd with polynomials* p *for which* f *divides* p. *However,* $\deg(f') < \deg(f)$, *and thus* f *can't divide* f'.

Exercise 4.2. *Let* $\mathrm{char}(K) = p > 0$. *Then:*

1. *Let* L/K *be a finite field extension, and let* $\mathrm{char}(K) = p$. *Prove that* L *is a separable extension if* $[L : K]$ *is relatively prime to* p.

2. *Prove that* a *has a* p^{th} *root in* k *iff* $X^{p^n} - a$ *is not irreducible over* k *for any* $n \in \mathbb{N}$.

3. *Let* $\alpha \in \overline{k}$. α *is separable over* k *iff* $k(\alpha) = k(\alpha^{p^n})$ *for all* $n \in \mathbb{N}$.

4. k *is perfect iff every element of* k *has a* p^{th} *root in* k, *i.e.* $k = k^p$, *where* $k^p := \{x^p : x \in k\}$ *is the image of* k *under the Frobenius map. Recall that a field* k *is said to be perfect if* $\overline{k}/k$ *is separable.*

Proof. The proofs are as follows:

1. Write $n := [L : K]$, and let $\alpha \in L$. Then $\deg_K(\alpha) \mid n$, and thus $\deg_K(\alpha)$ is relatively prime to p. Consequently, if $f(X) = X^d + \cdots$ is the minimal polynomial of α over K, then $f'(X) = dX^{d-1} + \cdots \neq 0$. Since $f'(X) \neq 0$, $f(X)$ and $f'(X)$ are co-prime, and consequently, all roots of f are distinct.

2. Let $\alpha_n \in \overline{k}$ be such that $\alpha_n^{p^n} = a$. Then $X^{p^n} - a = (X - \alpha_n)^{p^n}$, i.e. $X^{p^n} - a$ has exactly one root in $\overline{k}$.
Now, if $a = b^p$ for some $b \in k$, then $X^{p^n} - a = (X^{p^{n-1}} - b)^p$, and thus $X^{p^n} - a$ is not irreducible over k for any $n \in \mathbb{N}$.
Conversely, suppose $f(X) := X^{p^n} - a$ is not irreducible over k. Let $g(X)$ be the minimal polynomial of α_n over k,

and let $f(X) = g(X)^m h(X)$, where $g(X) \nmid h(X)$. Since $g(X)$ is the minimal polynomial, $m \geq 1$. However, note that the only root f has is α_n, and consequently, the only root h has is α_n. However, any polynomial over $k[X]$ which has α_n as a root must be divisible by $g(X)$, which is a contradiction, and thus $f(X) = g(X)^m$. Comparing degrees leads to $m = p^{n-u}, \deg(g) = p^u$ for some $u \leq n-1$. Note that $u \neq n$ since f is not irreducible. Also note that $g(X) = (X - \alpha_n)^{p^u} = X^{p^u} - \alpha_n^{p^u}$, and thus $\alpha_n^{p^u} \in k$, since $g(X) \in k[X]$. Set $b := (\alpha_n^{p^u})^{p^{n-1-u}} = \alpha^{p^{n-1}} \in k$. Clearly, $b^p = a$, as desired.

3. Let f be the minimal polynomial of α over k.
   Suppose α is not separable, i.e. f is not separable. Then by Exercise 4.1, $f(X) = g(X^p)$ for some irreducible polynomial $g(X) \in k[X]$, and consequently, $\deg_k(\alpha^p) = \deg_k(\alpha)/p$, which implies that $\deg_k(\alpha^p) \neq \deg_k(\alpha)$. But then $k(\alpha^p) \neq k(\alpha)$, since $[k(\alpha^p) : k] = \deg_k(\alpha^p) \neq \deg_k(\alpha) = [k(\alpha) : k]$.
   Conversely, suppose α is separable. Let $r(X) \in k(\alpha^{p^n})[X]$ be the minimal polynomial of α over $k(\alpha^{p^n})$. Now, note that α satisfies $X^{p^n} - \alpha^{p^n} \in k(\alpha^{p^n})[X]$, and consequently, $r(X) \mid X^{p^n} - \alpha^{p^n}$. But note that $X^{p^n} - \alpha^{p^n}$ has a single root in $\overline{k}$, and consequently, r also has a single root in $\overline{k}$. Furthermore, since α is separable over k, it is also separable over $k(\alpha^{p^n})$. Consequently, the degree of r must be 1. But that implies that $\alpha \in k(\alpha^{p^n})$, which implies $k(\alpha^{p^n}) = k(\alpha)$, as desired.

4. Suppose k is perfect. For any $a \in k$, consider the polynomial $f(X) := X^p - a \in k[X]$. Note that $f(X)$ has the unique root $a^{1/p} \in \overline{k}$, and thus if $a^{1/p} \notin k$, then the algebraic extension $k(a^{1/p})/k$ wouldn't be separable, leading to a contradiction.
   Conversely, suppose every element of k has a p^{th} root. Let $f(X) \in k[X]$ be an irreducible polynomial that is not separable. Then $f(X) = g(X^p)$ for some polynomial $g \in k[X]$. But

$$f(X) = g(X^p) = \sum a_i (X^p)^i = \left(\sum a_i^{1/p} X^i \right)^p$$

   This contradicts the fact that f was irreducible over k.

□

Remark: By the p^{th} root condition, it is easy to see that if F is a characteristic p field, then the largest perfect subfield of F is $\bigcap_{i=0}^{\infty} F^{p^i}$.

Exercise 4.3. *Let k be a field of characteristic p. Let $\alpha \in \overline{k}$ be separable, and let $\alpha_1, \ldots, \alpha_d$ be the conjugates of α, i.e. $\alpha_1, \ldots, \alpha_d$ are the roots of the minimal polynomial of α over k. Prove that $\alpha_1^{p^n}, \ldots, \alpha_d^{p^n}$ are the conjugates of α^{p^n}.*

Proof. Let $f(X) = \sum_{i=0}^{d} a_i X^i \in k[X]$ be the minimal polynomial of α over k (note that $a_d = 1$). Then $f(X)$ has $\alpha_1, \ldots, \alpha_d$ as its roots. Now, we claim that

$$g(X) = \sum_{i=0}^{d} a_i^{p^n} X^i$$

has $\alpha_1^{p^n}, \alpha_2^{p^n}, \ldots, \alpha_d^{p^n}$ as its roots. Indeed,

$$(-1)^{d-i} \frac{a_i}{a_d} = \sum_{S \in \binom{[n]}{d-i}} \prod_{j \in S} \alpha_j$$

Thus,

$$\sum_{S\in\binom{[n]}{d-i}}\prod_{j\in S}\alpha_j^{p^n} = \left(\sum_{S\in\binom{[n]}{d-i}}\prod_{j\in S}\alpha_j\right)^{p^n} = ((-1)^{p^n})^{d-i}\frac{a_i^{p^n}}{a_d^{p^n}}$$

For odd p, $(-1)^{p^n} = -1$. For $p = 2$, $-1 = 1$. In either case, we're done.
Consequently, $\deg_k(\alpha^{p^n}) \leq d$. At the same time, since α is separable, $k(\alpha) = k(\alpha^{p^n})$, which means $d = \deg_k(\alpha) = \deg_k(\alpha^{p^n})$, and consequently $g(X)$ is the minimal polynomial of α^{p^n}. But that means that the conjugates of α^{p^n} are $\alpha_1^{p^n}, \ldots, \alpha_d^{p^n}$, as desired. □

Exercise 4.4. *f is irreducible over k. $h(X) = f(X^{p^n})$ has a root β which is separable over k. Show that $h(X) = f_1(X)^{p^n}$ for some $f_1(X) \in k[X]$.*

Proof. Let $\beta_1, \ldots, \beta_r$ be the conjugates of β. By the previous exercise, $\beta_1^{p^n}, \ldots, \beta_r^{p^n}$ are the conjugates of β^{p^n}. Consequently,

$$\operatorname{irr}(\beta^{p^n}, k) = \prod_{i=1}^{r}(X - \beta_i^{p^n})$$

Then

$$h(X) = f(X^{p^n}) = \prod_{i=1}^{r}(X^{p^n} - \beta_i^{p^n}) = \left(\prod_{i=1}^{r}(X - \beta_i)\right)^{p^n} = \operatorname{irr}(\beta, k)^{p^n}$$

□

Exercise 4.5. *Consider the field extension $k(X, Y)/k(X^p, Y^p)$, where $\operatorname{char}(k) = p$. Prove that:*

1. *The degree of the extension is p^2.*
2. *There are infinitely many intermediate fields between $k(X^p, Y^p)$ and $k(X, Y)$. Consequently, by the Primitive Element Theorem, $k(X, Y)$ is not simple over $k(X^p, Y^p)$.*

Proof. Note that $k(X^p, Y^p) \subset k(X, Y^p) \subset k(X, Y)$. The degree of both the extensions is p, and thus the total degree is p^2. Indeed, $[k(X, Y) : k(X, Y^p)] = p$: Indeed, Y is a root of $T^p - Y^p \in k(X, Y^p)[T]$. By Gauss's lemma, it is enough to show the irreducibility of $T^p - Y^p \in k[X, Y^p][T]$. But note that Y^p is a prime element in $k[X, Y^p]$, and consequently, by Eisenstein's criterion, $T^p - Y^p$ is irreducible. The proof of the fact $[k(X, Y^p) : k(X^p, Y^p)] = p$ follows similarly.
We claim that $\{F(X + zY) : z \in F\}$ are all distinct intermediate fields, where $F := k(X^p, Y^p)$. Indeed, if $F(X + z_1Y) = F(X + z_2Y)$ (for $z_1 \neq z_2$), then $X + z_1Y \in F(X + z_2Y)$, which implies $Y \in F(X + z_1Y)$, which implies $X \in F(X + z_1Y)$, which implies $F(X + z_1Y) = k(X, Y)$. However, that can't be the case since $[F(X + z_1Y) : F] = p$, while $[k(X, Y) : F] = p^2$. To see why $[F(X+z_1Y) : F] = p$, note that $(X+z_1Y)^p = X^p + z_1^pY^p \in F$, and thus $\deg_F(X+z_1Y) \mid p$, implying $\deg_F(X+z_1Y) = 1, p$. But $\deg_F(X + z_1Y) \neq 1$, since that would imply $X + z_1Y \in F$, which can't be the case: Indeed, if

$$X + z_1Y = X + Y \cdot \frac{h(X, Y)}{\ell(X, Y)} = \frac{f(X, Y)}{g(X, Y)} \implies Xg(X, Y)\ell(X, Y) + Yh(X, Y)g(X, Y) = f(X, Y)\ell(X, Y)$$

Note that the degree of all terms on the RHS is divisible by p, while the LHS contains terms whose degrees are not divisible by p, leading to a contradiction. □

Exercise 4.6. *Let $k = \mathbb{F}_p(X, Y)$, and consider $h(T) := T^{p^2} + XT^p + Y \in k[T]$. Let β be a root of h in $\overline{k}$. Prove that:*

1. *β is not separable over k.*

2. *$[k(\beta) : k]_i = p$.*

3. *Let $E = k^{\text{insep}} \cap k(\beta)$. Then $E = k$.*

4. *One can not decompose the extension $k(\beta)/k$ into a separable and a purely inseparable extension.*

Proof. Note that $h(T)$ is irreducible: Indeed, it suffices to show its irreducibility in $\mathbb{F}_p[X,Y][T] \cong \mathbb{F}_p[X,T][Y]$, but h is a linear polynomial in $\mathbb{F}_p[X,T][Y]$, and hence irreducible. Since h is irreducible and monic, it is the minimal polynomial of β over k. Furthermore, $h'(T) = 0$. Thus, since $h(\beta) = h'(\beta) = 0$, β is not separable over k. Furthermore, $[k(\beta) : k] = p^2$.
Now, note that β^p is a root of $g(T) := T^p + XT + Y \in k[T]$, and furthermore, $g'(T) \neq 0$. Consequently, β^p is separable. Now, we claim that $k^{\text{sep}} \cap k(\beta) = k(\beta^p)$, i.e. the separable closure of k inside $k(\beta)$ equals $k(\beta^p)$. Indeed, note that $[k^{\text{sep}} \cap k(\beta) : k] = 1, p, p^2$, since $[k(\beta) : k] = p^2$. However, since β is not separable over k, $k(\beta)$ is not separable over k, and thus $[k^{\text{sep}} \cap k(\beta) : k] = 1, p$. At the same time, β^p is separable over k, and $\beta^p \notin k$ (since g is irreducible, and hence the minimal polynomial of β^p over k). Consequently, $[k^{\text{sep}} \cap k(\beta) : k] = p$, and thus $[k(\beta) : k]_s = p$, implying that $[k(\beta) : k]_i = p$.
Since $[k(\beta) : k]_s = p > 1$, $E \subsetneq k(\beta)$, and thus $[E : k] = 1, p$. Suppose $[E : k] = p$, and let $r := \text{irr}(\beta, E)$. Then $\deg(r) = [k(\beta) : E] = p$. Now, since $[E : k]_i = [E : k] = p$, $e^p \in k$ for all $e \in E$. Consequently, $r(T)^p \in k[T]$. Furthermore, $r(\beta)^p = 0$, and $\deg(r^p) = p^2$. Consequently, $r(T)^p = h(T)$. Now, if

$$r(T) := T^p + r_{p-1}T^{p-1} + \cdots + r_1 T + r_0 \implies h(T) = r(T^p) = T^{p^2} + r_{p-1}^p T^{p(p-1)} + \cdots + r_1^p T^p + r_0^p$$

Thus $r_0^p = Y, r_1^p = X$, and thus $X^{1/p}, Y^{1/p} \in E$, implying that $\mathbb{F}_p(X^{1/p}, Y^{1/p}) \subseteq E$. But by Exercise 4.5, $[\mathbb{F}_p(X^{1/p}, Y^{1/p}) : \mathbb{F}_p(X,Y)] = p^2$, which contradicts the fact that $[E : k] = p$. Thus $[E : k] = 1$, i.e. $E = k$.
Suppose $k(\beta)/k$ could be decomposed into $k(\beta)/F$, F/k, where $k(\beta)/F$ was separable, and F/k was purely inseparable. Since F/k is purely inseparable, $F \subseteq k^{\text{insep}} \cap k(\beta) = E = k$, and thus $F = k$. But $k(\beta)/F = k(\beta)/k$ is not separable. □

Exercise 4.7. *Let k be a field and let K/k be an algebraic extension such that every non-constant polynomial in k has a root in K. Then K is algebraically closed.*

Proof. Fix an algebraic closure $\overline{k}$, and WLOG assume $K \subseteq \overline{k}$. We will show that $K = \overline{k}$. It suffices to show that for every $\beta \in \overline{k}$, we have $\beta \in K$. Now, let $\beta_1, \ldots, \beta_n$ be the conjugates of β, and let $F := k(\beta_1, \ldots, \beta_n)$ be the splitting field of $\text{irr}(\beta, k)$ in $\overline{k}$. Since F/k is normal, we have $F = F_1 F_2$, where $F_1 := k^{\text{insep}} \cap F$, $F_2 := k^{\text{sep}} \cap F$. Consequently, it suffices to show that $F_1 \subseteq K, F_2 \subseteq K$. We now proceed case by case:

1. $F_1 \subset K$ is obvious: Indeed, if $\alpha \in F_1$, then $\text{irr}(\alpha, k) \in k[X]$ has α as a unique root in $\overline{k}$, which must belong to K by the problem hypothesis.

2. $F_2 \subset K$: Note that F_2/k is a finite separable field extension, and thus is simple by the primitive element theorem. Thus, let $F_2 = k(\gamma)$ for some $\gamma \in \overline{k}$. Now, if $\gamma_1, \ldots, \gamma_r$ are the conjugates of γ, then we claim that $k(\gamma_i) = k(\gamma)$: Indeed, note that F_2 is normal, and hence $\gamma_i \in F = k(\gamma) \implies k(\gamma_i) \subseteq k(\gamma)$. However, since γ_i is a conjugate of γ, $[k(\gamma_i) : k] = [k(\gamma) : k]$, and thus $k(\gamma_i) = k(\gamma)$. Now, consider $\text{irr}(\gamma, k) \in k[X]$. By the problem hypothesis, some root of this polynomial must lie in K, i.e. $\gamma_i \in K$ for some i, i.e. $k(\gamma_i) \subset K \iff F_2 \subset K$, as desired.

□

Exercise 4.8. *Prove that for every $a \in \mathbb{F}_p^\times$, $f(X) := X^p - X + a$ is irreducible over $\mathbb{F}_p$, and hence separable.*

Proof. Let $\alpha \in \overline{\mathbb{F}}_p$ be a root of $f(X)$. Then note that $\alpha + b$, where $b \in \mathbb{F}_p$, is also a root of f, since $b^p = b$. Now suppose $f(X) = g(X)h(X)$ for some $g \in \mathbb{F}_p[X]$, where $\deg(g) < p$. Then the roots of g are of the form $\alpha + b_1, \alpha + b_2, \ldots, \alpha + b_{\deg(g)}$. These roots sum up to $\alpha \cdot \deg(g) + b$ for some $b \in \mathbb{F}_p$, and since $g(X) \in \mathbb{F}_p[X]$, $\alpha \cdot \deg(g) + b \in \mathbb{F}_p$, implying that $\alpha \in \mathbb{F}_p$, since $\deg(g) < p$ is non-zero. But for any $x \in \mathbb{F}_p$, $x^p - x + a = a \neq 0$, which leads to a contradiction. □

Exercise 4.9. *Prove the following statements:*

1. $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ *iff* $d \mid n$.
2. *Let q be a prime power, and let $f(X) \in \mathbb{F}_q[X]$ be an irreducible polynomial of degree d. Then $d \mid n$ iff $f(X) \mid (X^{q^n} - X)$.*
3. *Let I_d be the set of all monic irreducible polynomials of degree d over $\mathbb{F}_q$. Then*

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in I_d} f(X)$$

4. *Given any $n \in \mathbb{N}$ and prime power q, there is a degree n irreducible polynomial over $\mathbb{F}_q$.*

Proof. The proofs are as follows:

1. Let α generate $\mathbb{F}_{p^d}^\times$, and β generate $\mathbb{F}_{p^n}^\times$. The order of α is $p^d - 1$, while the order of β is $p^n - 1$. Now, write $n = d\ell + k$, where $0 \leq k < d$. Then $p^d - 1$ divides $p^{d\ell} - 1$, and hence $p^n - p^k$.
   Now, suppose $d \nmid n$, and $(p^d - 1) \mid (p^n - 1)$. Then $(p^d - 1) \mid (p^k - 1)$, which is a contradiction since $0 < k < n$. But this also means that $\mathbb{F}_{p^d} \not\subset \mathbb{F}_{p^n}$, since if $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$, then α would have been a power of β, and the order of β would be divisible by the order of α.
   Conversely, suppose $d \mid n$. Then $(p^d - 1) \mid (p^n - 1)$, and consequently, $X^{p^n-1} - 1 = (X^{p^d-1})^t - 1$, where $t := (p^n - 1)/(p^d - 1)$. But $X^{p^d-1} - 1$ divides $(X^{p^d-1})^t - 1$, and consequently, all roots of $X^{p^d-1} - 1$ can be found in $\mathbb{F}_{p^n}$, which is the set of roots of $X^{p^n-1} - 1$. But we also know that the roots of $X^{p^d-1} - 1$ form a field isomorphic to $\mathbb{F}_{p^d}$, and thus we can take the roots of $X^{p^d-1} - 1$ to form a copy of $\mathbb{F}_{p^d}$ within $\mathbb{F}_{p^n}$.

2. Let E be the splitting field of f over $\mathbb{F}_q$. Note that $f(X) \mid (X^{q^n} - X)$ is equivalent to $E \subset \mathbb{F}_{q^n}$ [1]. Now, let α be some root of f, and consider the field $\mathbb{F}_q(\alpha)$. Since $\mathbb{F}_q(\alpha)$ is an algebraic extension of $\mathbb{F}_q$, it is normal (we use Exercise 3.7 to conclude this). Since α is the root of an irreducible polynomial f, $\mathbb{F}_q(\alpha)$ contains all roots of f, and thus $\mathbb{F}_q(\alpha) \supseteq E$. At the same time, $E \supseteq \mathbb{F}_q(\alpha)$, since E contains all roots of f. Thus $E = \mathbb{F}_q(\alpha)$, and $[E : \mathbb{F}_q] = \deg_{\mathbb{F}_q}(\alpha) = \deg(f) = d$.
   Now, if $E \subset \mathbb{F}_{q^n}$, then $[E : \mathbb{F}_q] \mid [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, and consequently, $d \mid n$.
   Conversely, assume $d \mid n$. As above, $[E : \mathbb{F}_q] = d$, and thus E is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_{q^d}$. Since $d \mid n$, $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, and consequently, $E \subseteq \mathbb{F}_{q^n}$, as desired.

3. Note that for any $d \mid n$, and any $f \in I_d$, $f(X) \mid X^{q^n} - X$. Furthermore, since all polynomials in the I_d's are irreducible over $\mathbb{F}_q$, they are co-prime. Consequently, the product of all polynomials in I_d for all $d \mid n$ must divide $X^{q^n} - X$.
   Now, every element in $\mathbb{F}_{q^n}$ is algebraic over $\mathbb{F}_q$, and hence has a minimal polynomial over $\mathbb{F}_q$. Furthermore, the degree of the minimal polynomial must divide n, since $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Thus, $X^{q^n} - X$, which equals $\prod_{\alpha \in \mathbb{F}_{q^n}} (X - \alpha)$, must divide $\prod_{d|n} \prod_{f \in I_d} f(X)$, as can be seen by splitting both polynomials over $\overline{\mathbb{F}}_q$. Consequently, $X^{q^n} - X = \gamma \prod_{d|n} \prod_{f \in I_d} f(X)$ for some $\gamma \in \overline{\mathbb{F}}_q$. But note that all polynomials in I_* are monic, and hence $\gamma = 1$.

[1] WLOG assume both E and $\mathbb{F}_{q^n}$ to be subsets of $\overline{\mathbb{F}}_q$

4. Let $\ell(d) := d \cdot |I_d|$. Then $q^n = \sum_{d|n} \ell(d)$, which, by the Möbius inversion formula, implies that

$$\ell(n) = \sum_{d|n} \mu(n/d) q^d = q^n + \sum_{\substack{d|n \\ d \neq n}} \mu(n/d) q^d$$

But

$$\left| \sum_{\substack{d|n \\ d \neq n}} \mu(n/d) q^d \right| \leq \sum_{\substack{d|n \\ d \neq n}} q^d \leq \sum_{d=1}^{n-1} q^d = \frac{q^n - 1}{q - 1} < q^n$$

Consequently, $\ell(n) > 0$ for any $n \in \mathbb{N}$, as desired. Furthermore, since $\ell(n) = n \cdot |I_n|$, $\ell(n) \geq n$.

□

Remark: The above proofs were first given by Gauss.

Exercise 4.10. *Let* $\text{char}(k) = p > 0$*. A polynomial* $f(X) \in k[X]$ *is called a p-polynomial if it is of the form:*

$$f(X) = a_m X^{p^m} + a_{m-1} X^{p^{m-1}} + \cdots + a_1 X^p + a_0 X$$

Let F *be the splitting field of* f*, and let* A *be the set of roots of* f *in* F*. Prove that* f *is a p-polynomial if and only if* $(A, +_F, 0_F)$ *is an abelian group and all roots have the same multiplicity* p^e*.*

Proof. Note that

$$f(X) = a_m X^{p^m} + a_{m-1} X^{p^{m-1}} + \cdots + a_e X^{p^e} = a_m \left(X^{p^e}\right)^{p^{m-e}} + a_{m-1} \left(X^{p^e}\right)^{p^{m-1-e}} + \cdots + a_e X^{p^e} = g(X^{p^e})$$

where g is also a p-polynomial. Furthermore, $g'(X) = a_e \neq 0$, and thus g is separable, and consequently, all roots of f have the same multiplicity p^e. Furthermore, if r, s are roots of f, then for any $x, y \in \mathbb{F}_p$,

$$f(xr + ys) = \sum_{i=0} a_i (xr + ys)^{p^i} = \sum_{i=0} a_i (x^{p^i} r^{p^i} + y^{p^i} s^{p^i}) = \sum_{i=0} a_i (x r^{p^i} + y s^{p^i}) = x f(r) + y f(s) = 0$$

Consequently, the roots of f actually form a $\mathbb{F}_p$-vector space, which is obviously an abelian group.
Conversely, let A be a subgroup of the additive group of some field of characteristic p. Note that the order of every element of A is p, and thus by the structure theorem for abelian groups, $A \cong (\mathbb{Z}/p\mathbb{Z})^t \cong \mathbb{F}_p^t$ for some t, and thus A is a $\mathbb{F}_p$-vector space. We now induct on t. For $t = 1$, the roots are $0, \alpha, \ldots, (p-1)\alpha$ for some α. Note that $X^p - \alpha^{p-1} X$ has $k\alpha$ as roots for $0 \leq k < p$, and thus

$$\prod_{k=0}^{p-1} (X - k\alpha) = X^p - \alpha^{p-1} X$$

Clearly, $X^p - \alpha^{p-1} X$ is a p-polynomial. Now, suppose the statement is true up to $t = \ell - 1$, and we want to prove it for $t = \ell$. Thus, let $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ be the generators of A, and let $h(X)$ be the p-polynomial with roots in the subspace generated by $\alpha_1, \ldots, \alpha_{\ell-1}$. Now,

$$\prod_{k_1=0}^{p-1} \cdots \prod_{k_\ell=0}^{p-1} \left(X - \sum_{i=1}^{\ell} k_i \alpha_i \right) = \prod_{k_\ell=0}^{p-1} \prod_{k_1=0}^{p-1} \cdots \prod_{k_{\ell-1}=0}^{p-1} \left((X - k_\ell \alpha_\ell) - \sum_{i=1}^{\ell-1} k_i \alpha_i \right) = \prod_{k_\ell=0}^{p-1} h(X - k_\ell \alpha_\ell) = \prod_{k_\ell=0}^{p-1} (h(X) - k_\ell h(\alpha_\ell))$$

$$= h(X)^p - h(\alpha_\ell)^{p-1}h(X)$$

Since $h(X)$ is a p-polynomial, $h(X)^p - h(\alpha_\ell)^{p-1}h(X)$ is also a p-polynomial. Finally, if all roots have multiplicity p^e, our p-polynomial gets raised to power p^e. But raising a p-polynomial to power p^e gives another p-polynomial, so we're done. □

5 Galois Theory

Exercise 5.1. *Calculate the Galois groups of the following polynomials:*

1. $f(X) := X^3 - X - t$ *over* $\mathbb{C}(t)$.
2. $f(X) := X^3 + t^2X - t^3$ *over* $\mathbb{C}(t)$.
3. $f(X) := X^n - t$ *over* $\mathbb{C}(t)$.
4. $f(X) := (X^2 - p_1)\cdots(X^2 - p_n)$ *over* $\mathbb{Q}$, *where* $p_1, \dots, p_n$ *are distinct prime numbers.*
5. $f(X) := X^p - 2$ *over* $\mathbb{Q}$, *where* $p \geq 3$ *is a prime.*

Proof. The groups are as follows:

1. We first check the irreducibility of the polynomial over $\mathbb{C}(t)[X]$. By Gauss lemma, it is equivalent to checking irreducibility over $\mathbb{C}[t][X] \cong \mathbb{C}[X,t]$. But f is linear and monic over $\mathbb{C}[X,t]$, and hence irreducible. Now, the discriminant of f is $4 - 27t^2$. We claim that $4 - 27t^2$ is not a square in $\mathbb{C}(t)$. Indeed, if $p, q \in \mathbb{C}[t]$ ($\gcd(p,q) = 1$) are such that $p^2/q^2 = 4 - 27t^2$, then $q^2 \mid p^2$, which can't be, since $\gcd(p,q) = 1$, and thus q is constant. WLOG q is 1, and thus $p^2 = 4 - 27t^2$. Thus p is a linear polynomial, which leads to a contradiction on comparing coefficients.
   Thus the Galois group of f is $\mathfrak{S}_3$.

2. Put $X = ct$ to obtain $t^3(c^3 + c - 1) = 0$, and thus $f(X) = (X - \lambda_1 t)(X - \lambda_2 t)(X - \lambda_3 t)$, where $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$ are the roots of $c^3 + c - 1 = 0$. Thus f splits completely over $\mathbb{C}(t)$, and thus the Galois group is 0.

3. The splitting field of f is $\mathbb{C}(t^{1/n})$. Now, if $\sigma \in \mathrm{Gal}(\mathbb{C}(t^{1/n})/\mathbb{C}(t)) =: G$, then $\sigma(t^{1/n}) = t^{1/n}\zeta_n^{k_\sigma}$, where ζ_n is the n^{th} root of unity. Thus consider the map $G \mapsto \mathbb{Z}/n\mathbb{Z}$, $\sigma \mapsto k_\sigma$. This map is easily verified to be a group homomorphism, and it is injective since if $k_\sigma = 0$, then $\sigma = \mathrm{id}$. But $|G| = [\mathbb{C}(t^{1/n}) : \mathbb{C}(t)] = n$ (since $X^n - t$ is irreducible over $\mathbb{C}(t)[X]$), and thus the map is surjective, and hence an isomorphism. Thus $\mathrm{Gal}(\mathbb{C}(t^{1/n})/\mathbb{C}(t)) \cong \mathbb{Z}/n\mathbb{Z}$.

4. Let K/F be a finite Galois extension, and let $\alpha \in K$. Then $\mathrm{tr}_{K/F}(\alpha) := \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$. Note that tr is F-linear. Now, suppose F is a characteristic 0 field, and let $d \in F \setminus F^2$ be such that $\sqrt{d} \in K$. Then $\mathrm{tr}_{K/F}(\sqrt{d}) = 0$: Indeed, consider $\sigma \in \mathrm{Gal}(K/F)$. Then $\sigma(\sqrt{d}) = \pm\sqrt{d}$. Furthermore, $\sigma(\sqrt{d}) = \sqrt{d}$ if and only if $\sigma \in \mathrm{Gal}(K/F(\sqrt{d}))$. But $[K : F] = 2[K : F(\sqrt{d})]$, and thus exactly half of the automorphisms in $\mathrm{Gal}(K/F)$ map $\sqrt{d}$ to $\sqrt{d}$, and the other half map it to $-\sqrt{d}$, and thus the trace is 0, as desired.
   We now claim that $[E(\sqrt{p_{i+1}}) : E] = 2$, where $E := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_i}) = \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_i}]$. To show this, it is enough to show that $\sqrt{p_{i+1}} \notin E$. AFTSOC it is. Now, a typical element of E looks like $\sum_{S \subseteq [i]} a_S \sqrt{d_S}$, $d_S := \prod_{j \in S} p_j$. Note that $\sqrt{d_S} \notin \mathbb{Q}$ if $S \neq \emptyset$. Thus,

$$\sqrt{p_{i+1}} = \sum_{S \subseteq [i]} a_S \sqrt{d_S} \implies \mathrm{tr}_{E(\sqrt{p_{i+1}})/E}(\sqrt{p_{i+1}}) = \sum_{S \subseteq [i]} a_S \, \mathrm{tr}_{E(\sqrt{p_{i+1}})/E}(\sqrt{d_S}) \implies 0 = a_\emptyset$$

Now,

$$p_{i+1} = \sum_{S \neq \emptyset} a_S \sqrt{d_S p_{i+1}} \implies \operatorname{tr}_{E(\sqrt{p_{i+1}})/E}(p_{i+1}) = \sum_{S \subseteq [i]} a_S \operatorname{tr}_{E(\sqrt{p_{i+1}})/E}(\sqrt{d_S p_{i+1}}) \implies p_{i+1} \cdot |\operatorname{Gal}(E(\sqrt{p_{i+1}})/E)| = 0$$

which leads to a contradiction.
Thus, the desired Galois group (say G) has order 2^n. Now, let $\sigma \in G$. Then $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$ for all i, and thus $\sigma^2 = \mathrm{id}$. Thus G is a group where every element has order 2. Then by standard group theory, G is abelian. Thus, by structure theorem, G is isomorphic to the product of cyclic groups. Now, if the size of any of those cyclic groups is > 2, then G would have an element of order > 2. Thus, $\operatorname{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$.

5. The splitting field of f is $E := \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$. Now, consider the split short exact sequence:

$$1 \longrightarrow \operatorname{Gal}(E/\mathbb{Q}(\zeta_p)) \hookrightarrow \operatorname{Gal}(E/\mathbb{Q}) \twoheadrightarrow \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \longrightarrow 1$$

where the splitting $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \operatorname{Gal}(E/\mathbb{Q})$ is just an inclusion (where $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is extended to E by setting $\sigma(\sqrt[p]{2}) = \sqrt[p]{2}$). Thus, $\operatorname{Gal}(E/\mathbb{Q}) \cong \operatorname{Gal}(E/\mathbb{Q}(\zeta_p)) \rtimes \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. Now, note that $\operatorname{Gal}(f)$ is non-abelian: Indeed, define $\sigma, \tau \in \operatorname{Gal}(f)$ as $\sigma(\zeta_p) = \zeta_p^2, \sigma(\sqrt[p]{2}) = \sqrt[p]{2}, \tau(\zeta_p) = \zeta_p, \tau(\sqrt[p]{2}) = \sqrt[p]{2}\zeta_p$, and note that $\sigma\tau(\sqrt[p]{2}) = \sqrt[p]{2}\zeta_p^2 \neq \sqrt[p]{2}\zeta_p = \tau\sigma(\sqrt[p]{2}) \implies \sigma\tau \neq \tau\sigma$. We also claim that there is a unique non-abelian semi-direct product $\mathbb{Z}_p^\times \rtimes \mathbb{Z}_p$ (upto isomorphism): Indeed, non-abelian semi-direct products correspond to non-trivial homomorphisms $\mathbb{Z}_p^\times \longrightarrow \operatorname{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times$. Let G_1 be the semi-direct product corresponding to $\varphi^{(1)} : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$, and G_2 be the semi-direct product corresponding to $\varphi^{(2)} : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$. Suppose $\varphi^{(1)} = x \mapsto x\alpha$ (where $\gcd(\alpha, p-1) = 1$), where $x\alpha$ corresponds to the automorphism of $\mathbb{Z}_p$ as $y \mapsto x\alpha \cdot y$. Similarly, let $\varphi^{(2)} = x \mapsto x\alpha'$. Then the isomorphism ψ of $\mathbb{Z}_p^\times$ sending α to α' induces an isomorphism from G_1 to G_2: Indeed,

$$\psi((a,b) \cdot_{G_1} (c,d)) = \psi((a\varphi_b^{(1)}(c), bd)) := (\psi(a)\psi(\varphi_b^{(1)}(c)), \psi(b)\psi(d))$$

$$(\psi(a), \psi(b)) \cdot_{G_2} (\psi(c), \psi(d)) = (\psi(a)\varphi^{(2)}_{\psi(b)}(\psi(c)), \psi(b)\psi(d))$$

Thus, if we verify $\psi(\varphi_b^{(1)}(c)) = \varphi^{(2)}_{\psi(b)}(\psi(c))$, we're done. But $\psi(\varphi_b^{(1)}(c)) = \psi(bc\alpha) = \psi(b)\psi(c)\alpha'$, $\varphi^{(2)}_{\psi(b)}(\psi(c)) = \psi(b)\alpha' \cdot \psi(c)$, as desired.
Note that in particular, the non-abelian semi-direct product can be given by the identity $\varphi : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$. Thus $\operatorname{Gal}(f) = \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_p^\times$, where $\varphi : \mathbb{Z}_p^\times \longrightarrow \operatorname{Aut}(\mathbb{Z}_p)$ is the identity homomorphism.

□

Exercise 5.2. *Let $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ be an irreducible quartic with roots $\pm\alpha, \pm\beta$, where $\alpha, \beta \in \mathbb{C} \setminus \{0\}$. Let E be the splitting field of f. Prove that:*

1. $4 \leq [E : \mathbb{Q}] \leq 8$.
2. $\operatorname{Gal}(f) = D_8, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
3. $\operatorname{Gal}(f) = \mathbb{Z}/4\mathbb{Z}$ *if* $\alpha/\beta - \beta/\alpha \in \mathbb{Q}$.
4. $\operatorname{Gal}(f) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if* $\alpha\beta \in \mathbb{Q}$.
5. $\operatorname{Gal}(f) = D_8$ *otherwise.*

Proof. 1. Since f is irreducible, $\mathbb{Q}[X]/(f(X))$ is a subfield of E, and thus $[E:\mathbb{Q}] \geq 4$. Moreover, since f is irreducible, $\mathrm{Gal}(f) \leq \mathfrak{S}_4$. Now, if $\sigma \in \mathrm{Gal}(f)$, then $\sigma(-\alpha) = -\sigma(\alpha), \sigma(-\beta) = -\sigma(\beta)$. The only permutations in $\mathfrak{S}_4$ satisfying these conditions are $\mathcal{G} := \{\mathrm{id}, (\alpha, -\alpha), (\beta, -\beta), (\alpha, -\alpha)\cdot(\beta, -\beta), (\alpha, \beta)\cdot(-\alpha, -\beta), (\alpha, \beta, -\alpha, -\beta), (\alpha, -\beta, -\alpha, \beta), (\alpha, -\beta)\cdot(\beta, -\alpha)\}$. Note that $\mathcal{G} \cong D_8$ (since $\mathcal{G}$ is a subgroup of $\mathfrak{S}_4$ of size 8, i.e. $\mathcal{G}$ is a 2-Sylow subgroup of $\mathfrak{S}_4$), and thus $\mathrm{Gal}(f) \leq D_8$, as desired.

2. Since $\mathrm{Gal}(f) \leq D_8$, and $|\mathrm{Gal}(f)| \geq 4$, $|\mathrm{Gal}(f)| = 4, 8$. The only groups of order 4 are $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the only group of order 8 which is also a subgroup of D_8 is of course D_8 itself.

3. Since $\alpha/\beta - \beta/\alpha \in \mathbb{Q}$, $\sigma(\alpha)/\sigma(\beta) - \sigma(\beta)/\sigma(\alpha) = \alpha/\beta - \beta/\alpha$. The only permutations which do that are $\{\mathrm{id}, (\alpha, -\alpha)\cdot(\beta, -\beta), (\alpha, \beta, -\alpha, -\beta), (\alpha, -\beta, -\alpha, \beta)\} =: G_1$. Since $|\mathrm{Gal}(f)| \geq 4$, we must have $\mathrm{Gal}(f) = G_1$. Furthermore, note that $(\alpha, \beta, -\alpha, -\beta) \in G_1$ has order 4. Thus $G_1 \cong \mathbb{Z}/4\mathbb{Z}$.

4. Since $\alpha\beta \in \mathbb{Q}$, $\sigma(\alpha\beta) = \alpha\beta$ for all $\sigma \in \mathrm{Gal}(f)$. The only permutations which do that are $\{\mathrm{id}, (\alpha, -\alpha)\cdot(\beta, -\beta), (\alpha, \beta)\cdot(-\alpha, -\beta), (\alpha, -\beta)\cdot(\beta, -\alpha)\} =: G_2$. Since $|\mathrm{Gal}(f)| \geq 4$, we must have $\mathrm{Gal}(f) = G_2$. Furthermore, note that every element in G_2 has order 2. Thus $G_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5. The only subgroups of $\mathcal{G}$ of size 4 are $G_1, G_2, \{\mathrm{id}, (\alpha, -\alpha)\cdot(\beta, -\beta), (\alpha, -\alpha), (\beta, -\beta)\} =: G_3$. Note that $\mathrm{Gal}(f) \neq G_1, G_2$, since they fix $\alpha/\beta - \beta/\alpha$ and $\alpha\beta$ respectively. $\mathrm{Gal}(f) \neq G_3$ either, since no element of G_3 takes α to β, and $\mathrm{Gal}(f)$ being the Galois group of an irreducible polynomial must act transitively on its roots. Consequently, $\mathrm{Gal}(f) \cong D_8$.

□

Exercise 5.3. *Let $f \in k[X]$ be an irreducible quartic such that $|\mathrm{Gal}(f)| = 8$. Then $\mathrm{Gal}(f) = D_8$.*

Proof. Note that $\mathrm{Gal}(f) \leq \mathfrak{S}_4$. A subgroup of $\mathfrak{S}_4$ of size 8 must be a 2-Sylow subgroup of $\mathfrak{S}_4$. Now, note that all Sylow subgroups of the same cardinality are isomorphic to each other (since they are conjugate to each other), and the 2-Sylow subgroups of $\mathfrak{S}_4$ are isomorphic to D_8, so we're done. □

Exercise 5.4. *Let p be a prime. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p such that f has exactly two non-real roots. Then the Galois group of f is $\mathfrak{S}_p$.*

Proof. Let $E/\mathbb{Q}$ be the splitting field of f. Note that $\mathbb{Q}[X]/(f(X))$ is a subfield of E with degree p. Consequently, $p \mid [E:\mathbb{Q}] \implies p \mid |\mathrm{Gal}_{\mathbb{Q}}(f)|$. Thus, by Cauchy's theorem, there exists an element of order p in $\mathrm{Gal}_{\mathbb{Q}}(f)$.
Also note that since f has exactly two non-real roots, they must be conjugates of each other. Then the automorphism $\iota \mapsto -\iota$ of $\mathbb{C}$ induces an order 2 automorphism of E over $\mathbb{Q}$, i.e. an automorphism which maps one non-real root to the other, and keeps all the real roots fixed. Thus, $\mathrm{Gal}_{\mathbb{Q}}(f)$ has an order 2 element. Furthermore, the order 2 element is actually a transposition, since it must map one non-real root to its conjugate (it is here that we use the fact that there are exactly two non-real roots: If there were more than two non-real roots, then the restriction of complex conjugation could have been a composition of > 1 transpositions).
Finally, also note that $\mathrm{Gal}_{\mathbb{Q}}(f) \leq \mathfrak{S}_p$. Now, since $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a p-cycle and a 2-cycle, it must actually be equal to $\mathfrak{S}_p$, as desired. □

Remark: Recall from group theory that $(12\ldots n), (ab)$ generate $\mathfrak{S}_n$ if and only if $\gcd(|a-b|, n) = 1$. In particular, if p is prime, then a p-cycle and a 2-cycle generate $\mathfrak{S}_p$.

Exercise 5.5. *Let E/k be a finite separable extension of degree p, where p is prime. Let $E = k(\theta)$, and let the conjugates of θ be $\theta = \theta_1, \ldots, \theta_p$. Suppose $\theta_2 \in k(\theta)$. Then E/k is Galois.*

Proof. Let $L = k(\theta_1, \ldots, \theta_p)$ be the normal closure of θ over k. Note that $p \mid [L : k]$, and thus $\mathrm{Gal}(L/k)$ has an element σ of order p by Cauchy's theorem. Note that σ is a p-cycle over $\theta_1, \ldots, \theta_p$, i.e. σ is a cyclic permutation on $\theta_{r_1}, \ldots, \theta_{r_p}$. Choose t such that $\sigma^t(\theta_1) = \theta_2$. Replace σ by σ^t. Now, since $\theta_2 \in E$, and $\deg_k(\theta_2) = p$. Thus $E = k(\theta_2)$. Now, $[\sigma(E) : k] = p$, and $\theta_2 \in \sigma(E)$, and thus $\sigma(E) = k(\theta_2) = E$. Similarly, $\theta_3 \in \sigma(E)$ (since $\theta_2 \in E$), implying $\theta_3 \in E$. Continuing, we get that $E = L$, as desired. □

Exercise 5.6. *Let $f(x) \in \mathbb{Q}[X]$ such that $\mathrm{Gal}_{\mathbb{Q}}(f) = \mathfrak{S}_n$, where $n = \deg(f) \geq 3$. Then:*

1. *f is irreducible.*
2. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\mathrm{id}\}$.
3. *$\alpha^n \notin \mathbb{Q}$ if $n \geq 4$.*

Proof. The proofs are as follows:

1. Let $f(X) = f_1(X)^{n_1} \cdots f_r(X)^{n_r}$ be the decomposition of f into irreducible polynomials, where $\deg(f_i) = d_i$. Note that the degree of the splitting field of f over $\mathbb{Q}$ is at most $d_1! d_2! \cdots d_r!$, which is strictly less than $n!$ unless $r = 1, n_r = 1$.
2. Let σ be a non-trivial $\mathbb{Q}$-automorphism of $\mathbb{Q}(\alpha)$. Then σ sends α to $\alpha_2 \neq \alpha$. Since $\alpha_2 \in \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, there exists $p(X) \in \mathbb{Q}[X]$ such that $\alpha_2 = p(\alpha)$. Now, pick any element τ in the Galois group of f such that $\tau(\alpha) = \alpha$. Then $\tau(\alpha_2) = \tau(p(\alpha)) = p(\tau(\alpha)) = \alpha_2$. But there are elements of $\mathfrak{S}_n$ which fix α yet move α_2, leading to a contradiction.
3. If $\alpha^n = q \in \mathbb{Q}$, then $p(\alpha) = 0$, where $p(X) := X^n - q$. Since p is a monic polynomial of degree n, p is the minimal polynomial of α. Now, the splitting field of p is $\mathbb{Q}(q^{1/n}, \zeta_n)$. But $[\mathbb{Q}(q^{1/n}) : \mathbb{Q}] = n$ (since p is irreducible), and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where $\phi(\cdot)$ is the Euler totient function. Thus $[\mathbb{Q}(q^{1/n}, \zeta_n) : \mathbb{Q}] \leq n\phi(n) \leq n(n-1) < n!$ for $n \geq 4$, which is a contradiction.

□

Exercise 5.7. *Let $f(X) \in k[X]$ where $k \subseteq \mathbb{R}$. Suppose f is irreducible over k, and suppose f has a non-real root of absolute value* 1*. Then if $f(\alpha) = 0$, then $f(1/\alpha) = 0$. Furthermore, f is of even degree.*

Proof. Suppose $f(\omega) = 1$, with $|\omega| = 1$. Then $f(\overline{\omega}) = 0$, since f has real coefficients. Suppose $f(\alpha) = 0$. Then there exists $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(\alpha) = \omega$. Also write $\beta := \sigma^{-1}(\overline{\omega})$. Then $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \omega \cdot \overline{\omega} = |\omega|^2 = 1$. Thus $\alpha\beta = 1$, i.e. $\beta = 1/\alpha$. Note that f doesn't have 1 as a root, since it is irreducible over k. Thus, the number of roots of f must be even (simply pair every root of f with its reciprocal). □

Exercise 5.8. *Let E/k be Galois, and let H be a subgroup of $G := \mathrm{Gal}(E/k)$ such that H maps F to itself. Show that H is the normalizer of* $\mathrm{Gal}(E/F)$ *in* $\mathrm{Gal}(E/k)$.

Proof. Note that $H = \{\sigma \in \mathrm{Gal}(E/k) : \sigma(F) \subseteq F\} = \{\sigma \in \mathrm{Gal}(E/k) : \sigma(F) = F\}$. Suppose $\sigma \in H$. For any $\tau \in \mathrm{Gal}(E/F)$, note that $\sigma(\tau(\sigma^{-1}(x))) = x$ for any $x \in F$. Thus $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(E/F) \implies H \subseteq N_G(\mathrm{Gal}(E/F))$. Conversely, suppose $\sigma \in N_G(\mathrm{Gal}(E/F))$. Let $x \in F, \tau \in \mathrm{Gal}(E/F)$ be arbitrary. Since $\sigma \in N_G(\mathrm{Gal}(E/F))$, $\sigma^{-1}\tau\sigma = \tau' \in \mathrm{Gal}(E/F)$, and thus $\tau\sigma x = \sigma\tau' x$. But $\tau' \in \mathrm{Gal}(E/F) \implies \tau' x = x$, and thus τ fixes $\sigma(x)$ for all $x \in F$, i.e. $\mathrm{Gal}(E/F)$ fixes $\sigma(x)$. Thus $\sigma(x) \in F$ by the Galois correspondence, i.e. $\sigma(F) \subseteq F \implies \sigma(F) = F$, as desired. □

Exercise 5.9. *Let E/k be finite Galois with $G := \mathrm{Gal}(E/k)$. Let a be an element such that $\{\sigma(a) : \sigma \in \mathrm{Gal}(E/k)\}$ is a k-basis of E. Let H be a subgroup of G, and let $F = E^H$. Let $\{H\tau\}$ be the right cosets of G over H. Define $S(H\tau) = \sum_{\sigma \in H\tau} \sigma(a)$. Then $\{S(H\tau)\}$ is a k-basis for F.*

Proof. Suppose $\{S(H\tau_i) : 1 \le i \le r\}$ is linearly dependent. Then

$$\sum_{i=1}^{r} \alpha_i S(H\tau_i) = 0 \implies \sum_{i=1}^{r} \sum_{\sigma \in H\tau_i} \alpha_i \sigma(a) = 0 \implies \alpha_i = 0$$

Furthermore, $[F : k] = r$, thus the aforementioned set is a basis. □

Exercise 5.10. *Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree ≥ 3. Let S be the set of roots of f in $\mathbb{C}$. Then S can't contain a non-trivial arithmetic progression.*

Proof. Since f is irreducible, it has distinct roots. Suppose $\alpha = (\alpha' + \alpha'')/2$, where $\alpha, \alpha', \alpha'' \in S$. Since $\mathrm{Gal}(f)$ acts transitively on S, for all $\beta \in S$, we have $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(\alpha) = \beta$, and thus $\beta = (\sigma(\alpha') + \sigma(\alpha''))/2$. Thus, every element of S is an average of two other elements of S. This is not possible: Indeed, let $\eta \in S$ have the largest real part. Then the line $x = \Re(\eta)$ has at least two other elements of S. Among those elements, take the element with the largest imaginary part. That can't be the average of any two other elements, leading to a contradiction. □

Exercise 5.11. *Prove that there doesn't exist a Galois field extension K/k such that* $\mathrm{Gal}(K/k) \cong \mathbb{R}$.

Proof. AFTSOC not. Choose $\alpha \in K \setminus k$, and let L be the normal closure of $k(\alpha)$ over k. Since L/k is a finite normal extension, $\mathrm{Gal}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/k)$ of finite index. Thus, if we can show that $\mathbb{R}$ has no proper subgroups of finite index, then we'd be done.
Indeed, suppose $H < \mathbb{R}$ such that $|\mathbb{R}/H| = n < \infty$. Choose $x \notin H$. Since the quotient group $\mathbb{R}/H$ has order n, $nx \in H$. Now, consider the set $\{x/n^k : k \in \mathbb{N}\}$. It is infinite, and since H has only finitely many cosets, we must have $x/n^{k_1} - x/n^{k_2} \in H$ for some $k_1, k_2 \in \mathbb{N}$ such that $k_2 > k_1$. But then we have $x(n^{k_2-k_1} - 1) \in H$. At the same time, $nx \in H \implies n^{k_2-k_1}x \in H$. But then $n^{k_2-k_1}x - x(n^{k_2-k_1} - 1) = x \in H$, which leads to a contradiction. □

Remark: The above proof works verbatim to show that $\mathrm{Gal}(K/k) \ncong G$, where G is a *divisible group*. Recall that an abelian group G is called divisible if for every $x \in G, x \neq 0$, and every $n \in \mathbb{N}$, there exists $y \in G$ such that $ny = x$.