Galois Theory - 5122GALO6Y

Yoav Eshel

March 17, 2021

Contents

1 Summary

21.3

Theorem. *Let $K \subset L \subset M$ be a tower of fields, X a K-basis for L and Y an L-basis for M. Then the set of elements xy with $x \in X$ and $y \in Y$ forms a K-basis for M and we have*

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

In particular, $K \subset M$ is finite if and only if $K \subset L$ and $L \subset M$ are finite

Proof. Let $c \in M$. Then c can be written uniquely as $c = \sum_{y \in Y} b_y \cdot y$ with coefficients $b_y \in L$ that are almost all 0. The elements $b_y \in L$ each have a unique representation as $b_y = \sum_{x \in X} a_{xy} \cdot x$ with coefficients $a_{xy} \in K$ that are almost all 0. Hence

$$c = \sum_{y \in Y} \sum_{x \in X} a_{xy} \cdot x \cdot y$$

and so c is a finite unique K-linear combination of the elements xy. Therefore $(x, y) \in X \times Y$ forms a basis for M over K.

Since $|X \times Y| = |X| \cdot |Y|$ it follows that

$$[M : K] = [M : L] \cdot [L : K].$$

Moreover, it follows that $X \times Y$ is finite if and only if X and Y are finite, since X and Y are non-empty. □

21.5

Theorem. *Let L/K be a field extension and take $\alpha \in L$. Then*

1. *If α is transcendental over k, then $K[\alpha] \simeq K[X]$ and $K(\alpha) \simeq K(x)$.*
2. *If α is algebraic over K then there exists a unique monic irreducible polynomial $f = f_K^\alpha \in K[x]$ that has α has a zero. In this case there is a field isomorphism*

$$\begin{aligned} K[X]/(f) &\simeq K(\alpha) \\ g \mod (f) &\mapsto g(\alpha) \end{aligned}$$

and the degree of $K(\alpha)$ over K is the degree of f.

Proof. Consider the ring homomorphism $\phi : K[x] \to L$ given by $f \mapsto f(\alpha)$. The image of ϕ is equal to $K[\alpha]$, and we have two possibilities.

If α is transcendental over K, then ϕ is injective, and we obtain an isomorphism $K[x] \xrightarrow{\sim} K[\alpha]$. The field of fractions $K(\alpha)$ is then isomorphic to $K(x)$.

If α is algebraic over K, then $\ker \phi$ is a non-trivial ideal of $K[x]$. Since $K[x]$ is a PID, there is a unique monic generator $f = f_K^\alpha \in K[x]$ of $\ker \phi$. This is the "smallest" monic polynomial in $K[x]$ that has α as a zero. The isomorphism theorem then gives an isomorphism $K[x]/(f_k^\alpha) \xrightarrow{\sim} K[\alpha] \subset L$ of integral domains. Hence (f_K^α) is a prime ideal in $K[x]$ and f_K^α is irreducible. Since a prime ideal $(f_K^\alpha) \neq 0$ is a PID is maximal, we have that $K[x]/(f_k^\alpha) \cong K[\alpha]$ is a field and therefore equal to $K(\alpha)$. Since every polynomial modulo f_K^α has a unique representative g; obtained through division with remainder by f_K^α. If $\deg f_K^\alpha = n$ then the residue classes of $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for $K[x]/(f_K^\alpha)$ over K. Therefore $[K(\alpha) : K] = n = \deg f_K^\alpha$. □

21.9

Theorem. *For a tower $M/L/K$ of fields, we have*

$$K \subset M \text{ is algebraic} \iff K \subset L \text{ and } L \subset M \text{ are algebraic.}$$

Proof. If $K \subset M$ is algebraic, then for any $\alpha \in L \subset M$ there exists a polynomial $f \in K[x]$ with $f(\alpha) = 0$ so L/K is algebraic. Similarly, for any $\alpha \in M$ there exists a polynomial in $f \in K[x] \subset L[x]$ with $f(\alpha) = 0$ so M/L is algebraic as well.

Suppose that $K \subset L$ and $L \subset M$ are algebraic extensions and let $c \in M$. Then c has a minimum polynomial $f_L^c = \sum_{i=0}^n b_i x^i \in L[x]$. Each $b_i \in L$ is algebraic over K, so $L_0 = K(b_0, \ldots, b_n)$ is a finite extension of K. Because c is also algebraic over L_0, the extension $L_0(c)/L_0$ is finite. Since

$$[L_0(c) : K] = [L_0(c) : L_0] \cdot [L_0 : K]$$

the extension $L_0(c)/K$ is also finite and so algebraic. In particular, c is algebraic over K and so M/K is algebraic. □

22.1

Theorem. *Let F be a finite field and $\mathbb{F}_p$ the prime field of F. Then F is an extension of $\mathbb{F}_p$ of finite degree n , and F has p^n elements.*
Conversely, for any prime power $q = p^n$, there exists, up to isomorphism, a unique field $\mathbb{F}_q$ with q elements; it is the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Proof. If F is finite, then F is of finite degree over its prime field $\mathbb{F}_p$. If this degree is equal to n, then F, as an n-dimensional vector space over $\mathbb{F}_p$ has exactly p^n elements. THe group of units F^* then has order $p-1$ and it follows that the elements of F^* are exactly the $p^n - 1$ zeros of the polynomial $x^{p^n-1} - 1 \in F[x]$. In particular we have

$$\prod_{\alpha \in F} (x - \alpha) = x^{p^n} - x \in \mathbb{F}_p[x].$$

It follows that F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ and since splitting fields are unique (up to isomorphism), it follows there can exists at most one field with p^n elements.

Conversely, for every prime power $q = p^n > 1$, a splitting field of $f(x) = x^q - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$ is a field with q elements. Since $f' = -1$ has no zeros, f has no double roots in an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The zero set

$$\mathbb{F}_q = \{a \in \overline{\mathbb{F}_p} \mid a^{p^n} = \alpha\}$$

of f therefore has $q = p^n$ elements. By Fermat's little theorem, we have $\mathbb{F}_p \subset \mathbb{F}_q$. It is clear the $\mathbb{F}_q$ is closed under multiplication and division by non-zero elements. The additivity of taking pth power implies

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \in \mathbb{F}_q$$

and so $\mathbb{F}_q$ is closed under addition. It follows that F_q is a subfield of $\overline{\mathbb{F}_p}$ and therefore a splitting field of f over $\mathbb{F}_p$. □

22.10

Theorem. *Let $\mathbb{F}_q$ and $\mathbb{F}_r$ be subfields of $\overline{\mathbb{F}_p}$ with, respectively, $q = p^i$ and $r = p^j$ elements. The following are equivalent:*

1. *$\mathbb{F}_q$ is a subfield of $\mathbb{F}_r$.*
2. *r is a power of q.*
3. *i is divisor of j.*

Proof. If $\mathbb{F}_r$ is an extension field of $\mathbb{F}_q$ of degree d, then we have $r = q^d$ and therefore $j = di$. This proves $1 \implies 2 \implies 3$. Finally, if i is a divisor of j, then for $\alpha \in \overline{\mathbb{F}_p}$ we have the implication $\mathrm{Frob}_p^i(\alpha) = \alpha \implies \mathrm{Frob}_p^j(\alpha) = \alpha$. This is equivalent to $\mathbb{F}_q \subset \mathbb{F}_r$. □

23.1

Theorem. *Let $K \subset L_1 = K(\alpha)$ be a simple algebraic field extension, $K \subset L_2$ an arbitrary field extension and S the set of zeros of f_K^α in L_1. Then there is a bijection $Hom_K(L_1, L_2) \xrightarrow{\sim} S$ given by $\sigma \mapsto \sigma(\alpha)$.*

Proof. A homomorphism $\sigma : K(\alpha) \to L_2$ that is the identity on K is fixed by the choice of the elements $\sigma(\alpha) \in L_2$. To the $\sigma(\alpha)$ is a zero of $f = f_K^\alpha$ in L_2, we write $f = \sum_{i=0}^n a_i x^i \in K[x]$. Then

$$f(\sigma(\alpha)) = \sum_{i=0}^n a_i \sigma(\alpha)^i = \sigma\left(\sum_{i=0}^n a_i \alpha^i\right) = \sigma(f(\alpha)) = 0$$

because σ is the identity on $a_i \in K$. This proves $\sigma(\alpha) \in S$.

Conversely, for every zero $s \in S$ of f, the map $L_1 \to L_2$ defined by $\sum_i c_i \alpha^i \mapsto c_i s^i$ is a K-homomorphism $L_1 \to L_2$ □

23.5

Theorem. *For a finite extension $K \subset L$, the following are equivalent*

1. *The extension $K \subset L$ is separable*
2. *We have $L = K(\alpha_1, \ldots, \alpha_t)$ for elements $\alpha_1, \ldots, \alpha_t \in L$ that are separable over K*
3. *$[L : K]_s = [L : K]$*

Proof. (1 $\implies$ 2) Since L is a separable extension, every element in L is separable over K by definition. Moreover, since L is finite, it is algebraic, and so we can find $\alpha_1, \ldots, \alpha_t \in L$ that do the trick.

(2 $\implies$ 3) We know that for a simple extension $K(\alpha_i)$ it holds that

$$|[K(\alpha_i) : K]_s| = |\{\alpha \in L \mid f_K^{\alpha_i}(\alpha) = 0\}|$$

and since α_i is separable $f_K^{\alpha_i}$ has no repeated roots and so

$$|[K(\alpha_i) : K]_s| = |\{\alpha \in L \mid f_K^{\alpha_i}(\alpha) = 0\}| = \deg f_K^{\alpha_i} = [K(\alpha_i) : K].$$

Let $E = K(\alpha_1, \ldots, \alpha_k)$ for some $k \geq 1$ and suppose that

$$[E : K]_s = [E : K].$$

Then α_{k+1} is separable over E since $f_E^{\alpha_{k+1}} \mid f_K^{\alpha_{k+1}}$ in $\overline{K}[x]$. Therefore

$$[E(\alpha_{k+1}) : K]_s = [E(\alpha_{k+1}) : K]$$

which completes the induction.

(3 $\implies$ 1) For every $\alpha \in L$ we have a tower $K \subset K(\alpha) \subset L$. Since the separable degree is bounded by the degree, it follows from the equality

$$[L : K(\alpha)]_s \cdot [K(\alpha) : K]_s = [L : K]_s = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$$

that $[K(\alpha) : K]_s = [K(\alpha) : K]$. Therefore f_K^α has exactly $\deg f_K^\alpha$ distinct roots in $\overline{K}$, so α is separable over K. □

23.6

Theorem. *Let $f \in K[x]$ be an irreducible polynomial, and suppose that f is inseparable. Then we have $p = \operatorname{char} K > 0$ and $f = g(x^p)$ for some $g \in K[x]$. Moreover, not all coefficients of f are pth powers in K.*

Proof. If f has a double zero $\alpha \in \overline{K}$, then α is also a zero of the derivative of f' of f. Because (up to multiplication by a unit) f is the minimum polynomial of α over K, the assumption $f'(\alpha) = 0$ implies $f \mid f'$. Since f' has a lower degree than f, this is only possible if f' is the zero polynomial in $K[x]$.

For K of characteristic 0, we find that f is constant, which contradicts the assumption that f is irreducible. We therefore have char $K = p > 0$, and by explicitly taking derivatives we see that we obtain $f' = 0$ for the polynomials in $K[x]$ of the form $f = \sum_i a_i x^{ip} \in K[x]$. For $g = \sum_i a_i x^i$ we have $f = g(x^p)$.

If all coefficients of f are pth powers in K, say $a_i = c_i^p \in K$, then we have

$$f = \sum_i a_i x^{ip} = \sum_i c_i^p x^{ip} = \left(\sum_i c_i x^i \right)^p$$

which is a contradiction since f is irreducible. □

23.14

Theorem. *For a finite extension $K \subset L$ with fundamental set $X(L/K)$, the following are equivalent:*

1. *The extension $K \subset L$ is normal*
2. *The filed L is the splitting field Ω_K^f of a polynomial $f \in K[x]$.*
3. *For all $\tau, \sigma \in X(L/K)$, we have $\sigma[L] = \tau[L]$.*

Proof. (1 $\implies$ 2). Write $L = K(\beta_1, \ldots, \beta_t)$. Then because of the normality of $K \subset L$, all the zeros of

$$f = f_K^{\beta_1} \cdot f_K^{\beta_2} \cdots f_K^{\beta_t} \in K[x]$$

are in L. Since they generate L over K, we have $L = \Omega_K^f$.

(2 $\implies$ 3). Let $L = \Omega_K^f$ and suppose that in $\overline{K}[x]$, the polynomial f decomposes as $f = \prod_{i=1}^n (x - \alpha_i)$. This gives an inclusion $\sigma : L = K(\alpha_1, \ldots, \alpha_n) \subset \overline{K}$. For $\tau \in X(L/K)$ arbitrary, we then have $\prod_{i=1}^n (x - \tau(\alpha_i)) = f$ because τ is the identity on the coefficients of f. We find the τ permutes the zeros of f, and that given the desired equality $\tau[L] = K(\tau(\alpha_1), \ldots, \tau(\alpha_n)) = K(\alpha_1, \ldots, \alpha_n) = \sigma[L] \subset \overline{K}$.

(3 $\implies$ 1). Choose an element $\sigma : L \to \overline{K}$ in $X(L/K)$ and take $\alpha \in L$ arbitrary. Suppose that f_K^α decomposes as $f_K^\alpha = \prod_{i=1}^n (x - \alpha_i) \in \overline{K}[x]$. Then we have a K-isomorphism $\sigma_i : K(\alpha) \to K(\alpha_i) \subset \overline{K}$. Then each of the isomorphism σ_i has an extension to an isomorphism $\sigma_i' : \overline{L} \to \overline{K}$ where $\overline{L}$ is an algebraic closure of L (and therefore of $K(\alpha)$). This isomorphism maps α to $\alpha_i \in \sigma_i'[L]$, and by assumption 3, we have $\sigma_i'[L] = \sigma[L]$ for all σ_i'. It follows that f_K^α decomposes into linear factors over $\sigma[L][x]$ and therefore over $L[x]$. □

2 Introduction

Galois theory is about studying Polynomials with coefficients in a field ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.). Let

$$f(T) = T^n + \cdots + a_1 T + a_0 \in \mathbb{Q}[T].$$

Then $f(T)$ splits completely in $\mathbb{C}[T]$ as

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n)$$

with $\alpha_1, \ldots \alpha_n \in \mathbb{C}$ are the roots of f. Galois theory studies permutation of the the roots that preserve algebraic relations between these roots. The allowed permutation of the roots give rise to a group denoted $\mathrm{Gal}(f)$. The following definition of a Galois group does not require any background knowledge but is not very useful in practice.

Definition. *Let $\sigma : \mathbb{C} \to \mathbb{C}$ be a field automorphism and $\alpha \in \mathbb{C}$ a root of $F(T) \in \mathbb{Q}[T]$. Since $\sigma(1) = 1$ it follows that $\sigma(n) = n$ for all integers and so $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$ is the identity on $\mathbb{Q}$. Then*

$$\begin{aligned} f(\sigma(\alpha)) &= \sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(f(\alpha)) \\ &= 0. \end{aligned}$$

Then each automorphism σ is a permutation of the roots which is precisely the Galois group of the polynomial $Gal(f) \subset S_n$. In other words we have a group action

$$Aut(\mathbb{C}) \times \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$$

Then $Gal(f) := Im(\phi)$ where $\phi : Aut(\mathbb{C}) \to S_n$ mapping $\sigma \mapsto (\alpha_i \mapsto \sigma(\alpha_i))$

$\mathrm{Gal}(f) \subset S_n$ is transitive subgroup (i.e. if its action on the set of roots is transitive) if and only if f is irreducible.

3 Symmetric Polynomials

A symmetric polynomial is a polynomial $F(X_1, X_2, \ldots, X_n)$ the is invariant under permutations of its variables. In other words

$$P(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})$$

for all $\sigma \in S_n$. Symmetric polynomials arise naturally in the study of the relation between the roots of a polynomial in one variable and its coefficients, since the coefficients can be given by polynomial expressions in the roots, and all roots play a similar role in this setting. Let $f \in K(T)$ be a monic polynomial of degree n that splits completely in K. Then

$$f(T) = (T - X_1)(T - X_2) \cdots (T - X_n)$$

where X_i are the roots of f. Then

$$f(T) = T^n + s_1 T^{n-1} + \cdots + (-1)^n s_n$$

where

$$\begin{aligned} s_1 &= X_1 + X_2 + \cdots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\ &\vdots \\ s_n &= X_1X_2 \cdots X_n \end{aligned}$$

are called the *elementary symmetric polynomials* in $X_1, X_2, \dot{;} X_n$. Then the fundamental theorem of symmetric polynomials states that every symmetric polynomial can be written as a polynomial expression in the elementary symmetric polynomials.

To actually write a symmetric polynomial in terms of elementary symmetric polynomials we introduce some useful notation. We say a polynomial is ordered *lexicographically* if the monomial $T_1^{e_1}T_2^{e_2}\cdots T_n^{e_n}$ with the highest e_1 is in front. If two monomials have the same e_1, then we compare their e_2 and so on. Like a dictionary. If P is a symmetric polynomial in n variables, choose a single representative proceeded by the symbol $\sum_n$ to denote the sum over the monomials in the S_n orbit of the representative. Then for example

$$\begin{aligned} s_1 &= \sum_n T_1 \\ s_2 &= \sum_n T_1T_2 \\ &\vdots \\ s_n &= \sum_n T_1T_2\cdots T_n = T_1T_2\cdots T_n. \end{aligned}$$

Now suppose P is a symmetric polynomial. To find its representation in terms of symmetric polynomials:

1. Let $a \cdot T_1^{e_1}T_2^{e_2}\cdots T_n^{e_n}$ be the the first term in P, lexicographically.
2. Form the monomial
$$M = s_1^{e_1-e_2}s_2^{e_2-e_1}\cdots s_{n-1}^{e_{n-1}-e_n}s_n^{e_n}$$
3. Let $P_i = P - cM$.
4. Repeat steps (1)-(3) until $\deg P_i = 0$.
5. The we can solve for P and write it as a polynomial in the elementary symmetric polynomials.

The representation obtained through the algorithm above is unique.

The following theorem is useful when applying the algorithm above.

Theorem 1 (Orbit Stabilizer Theorem)**.** *Let G be a group acting on set S. For any $x \in S$ let $G_x = \{g \in G \mid g \cdot x = x\}$ denote the stabilizer of x, and let $G \cdot x = \{g \cdot x \mid g \in G\}$ denote the orbit of x. Then*

$$|G| = |G \cdot x||G_x|$$

Wondering how it might be useful? Consider

$$s_1^4 = \left(\sum_n T_1\right)^4 = (T_1 + \cdots + T_n)(T_1 + \cdots + T_n)(T_1 + \cdots + T_n)(T_1 + \cdots + T_n).$$

After some thinking you might conclude that there are five possible representatives:

$$T_1^4, \quad T_1^3 T_2, \quad T_1^2 T_2^2, \quad T_1^2 T_2 T_3 \quad \text{and} \quad T_1 T_2 T_3 T_4$$

(note the the degrees always add up to four). But what are the coefficients? That's when the orbit-stabilizer theorem comes to the rescue. Let the permutation group S_4 act on the set of indices by permuting them. Then the coefficients in front of $\sum_n T_1^4$ is the size of the orbit of $(1, 1, 1, 1)$. Since every permutation in S_4 return the same sequence, the size of the orbit is $\frac{4!}{4!} = 1$. Then the coefficients in front of $\sum_n T_1^2 T_2^2$ is the size of the orbit of $(1, 1, 2, 2)$. The permutations that fix it are $(1), (12), (34)$ and $(12)(34)$. So the size of the stabilizer is 4 and the size of the orbit is $\frac{4!}{4} = 6$ Similarly, the coefficients in front of $\sum_n T_1^2 T_2 T_3$ is the size of the orbit of $(1, 1, 2, 3)$. Since the stabilizer contains only the permutations that switches the 1s and fixes the other two elements (namely (1) and (12)) the size of the orbit is $\frac{4!}{2} = 12$. Lastly, the size of the orbit of $\sum_n T_1 T_2 T_3 T_4$ is the 4! since there is no permutations (except the identity of course) that stabilizes it. We conclude that

$$s_1^4 = \sum_n T_1^4 + 6 \sum_n T_1^2 T_2^2 + 12 \sum_n T_1^2 T_2 T_3 + 24 \sum_n T_1 T_2 T_3 T_4$$

4 Field Extensions

Prime Fields

Definition. *Let K be a field. Then the **prime field** in K is the intersection over all subfields of K*

Lemma 2. *Let K be a field of characteristic k. Then the prime field of K is $\mathbb{F}_p$ if $k = p$ and $\mathbb{Q}$ if $k = 0$.*

Algebraic and Transcendental Extensions

Let L/K be a field extensions. Then we say that $\alpha \in L$ is *algebraic* over K if there exists an $f \in K[x], f \neq 0$, such that $f(\alpha) = 0$. We say that α is *transcendental* over K if there exists no such f. The number of algebraic elements over $\mathbb{Q}$ in $\mathbb{C}$ is countable, so in fact $\mathbb{C}$ is mostly transcendental elements.

Definition. *We say that an extension L/K is **algebraic** if $\forall \alpha \in L$, α is algebraic over K.*

Lemma 3. *If a field extension is finite then it is algebraic.*

The converse of this lemma does not hold.

5 Exercises

Symmetric Polynomial

Exercise 14.10
Express the symmetric polynomials $\sum_n T_1^2 T_2$ and $\sum_n T_1^3 T_2$ in the elementary symmetric polynomials.

Solution. To get the polynomial $\sum_n T_1^2 T_2$ we start with

$$s_1 s_2 = \sum_n T_1 \sum_n T_1 T_2 = \sum_n T_1^2 T_2 + 3 \sum_n T_1 T_2 T_3 = \sum_n T_1^2 T_2 + 3 s_3$$

Thus

$$\sum_n T_1^2 T_2 = s_1 s_2 - 3 s_3$$

Similarly, to transform the polynomial $\sum_n T_1^3 T_2$ we start with

$$\begin{aligned} s_1^2 s_2 &= \left(\sum_n T_1 \right)^2 \sum_n T_1 T_2 \\ &= \left(\sum_n T_1^2 + 2 \sum_n T_1 T_2 \right) \sum_n T_1 T_2 \\ &= \sum_n T_1^2 \sum_n T_1 T_2 + 2 s_2^2 \\ &= \sum_n T_1^3 T_2 + \sum_n T_1^2 T_2 T_3 + 2 s_2^2. \end{aligned}$$

And since

$$s_1 s_3 = \sum_n T_1 \sum_n T_1 T_2 T_3 = \sum_n T_1^2 T_2 T_3 + 4 \sum_n T_1 T_2 T_3 T_4$$

it follows that $\sum_n T_1^2 T_2 T_3 = s_1 s_3 - 4 s_4$ and so

$$\sum_n T_1^3 T_2 = s_1^2 s_2 - s_1 s_3 + 4 s_4 - 2 s_2^2$$

Exercise 14.14
Prove: For $n \in \mathbb{Z}_{>0}$, we have $\Delta(X^n + a) = (-1)^{\frac{1}{2} n(n-1)} n^n a^{n-1}$.

Proof. Let $f(X) = X^n + a$ and let α_i be its roots. Then $f'(X) = n X^{n-1}$ and

$$\Delta(f) = (-1)^{n(n-1)/2} R(f, f').$$

Let $f_1(X) = a$ and then $f \equiv f_1 \mod (f')$ since $f = f_1 + f' \cdot \left(\frac{1}{n}X\right)$. Simplifying the resultant we get

$$\begin{aligned} R(f, f') &= R(f', f) && \text{(Property 1)} \\ &= n^n R(f', f_1) && \text{(Property 3)} \\ &= n^n \cdot \left(n^0 \prod_{i=1}^{n-1} f_1(\alpha_i) \right) && \text{(Property 2)} \\ &= n^n a^{n-1} \end{aligned}$$

and the result follows. □

Exercise 14.15
Calculate the discriminant of the polynomial $f(X) = X^4 + pX + q \in \mathbb{Q}(p, q)[X]$.

Solution. Then $f'(X) = 4X^3 + p$ and so

$$f_1(X) = f - f' \cdot h = X^4 + pX + q + (4X^3 + p)(\frac{1}{4}X) = \frac{3p}{4}X + q.$$

Then the resultant is

$$\begin{aligned} R(f, f') &= R(f', f) && \text{(Property 1)} \\ &= 4^{4-1} R(f', f_1) && \text{(Property 3)} \\ &= 4^3 \left((-1)^{3 \cdot 1} R(f_1, f') \right) && \text{(Property 1)} \\ &= -4^3 \left(\left(\frac{3p}{4} \right)^3 \prod_{i=1}^{1} f' \left(\frac{-4q}{3p} \right) \right) && \text{(Property 2)} \\ &= -3^3 p^3 \left(4 \left(\frac{-4q}{3p} \right)^3 + p \right) \\ &= 4^4 q^3 - 3^3 p^4. \end{aligned}$$

Therefore the discriminant of f is

$$\Delta(f) = (-1)^{4 \cdot 3/2} R(f, f') = R(f, f') = 4^4 q^3 - 3^3 p^4.$$

Exercise 14.16
For every $n > 1$, determine an expression for the discriminant of the polynomial $f(X) = X^n + pX + q \in \mathbb{Q}(p, q)[X]$.

Solution. Let $f(X) = X^n + pX + q \in \mathbb{Q}(p, q)[X]$ for $n > 1$. Then $f'(X) = nX^{n-1} + p$ and $f \equiv f_1 \mod (f')$ where

$$f_1 = f - f' \cdot h = X^n + pX + q - \left(nX^{n-1} + p \right) \left(\frac{1}{n} X \right) = \frac{p(n-1)}{n} X + q.$$

The resultant of f and f' is given by

$$\begin{aligned}
R(f,f') &= R(f',f) && \text{(Property 1)}\\
&= n^{n-1}R(f',f_1) && \text{(Property 3)}\\
&= n^{n-1}\left((-1)^{n-1}R(f_1,f')\right) && \text{(Property 1)}\\
&= (-n)^{n-1}\left(\frac{p(n-1)}{n}\right)^{n-1}\prod_{i=1}^{1} f'\left(-\frac{nq}{(n-1)p}\right) && \text{(Property 2)}\\
&= (-1)^{n-1}p^{n-1}(n-1)^{n-1}\left(\frac{(-1)^{n-1}n^nq^{n-1}}{(n-1)^{n-1}p^{n-1}}+p\right)\\
&= n^nq^{n-1}+(-1)^{n-1}p^n(n-1)^{n-1}.
\end{aligned}$$

Hence the discriminant of f is

$$\Delta(f) = (-1)^{n(n-1)/2}R(f,f') = (-1)^{n(n-1)/2}\left(n^nq^{n-1}+(-1)^{n-1}p^n(n-1)^{n-1}\right)$$

Exercise 14.17
Let $f \in \mathbb{Z}[X]$ be a monic polynomial. Prove that the following are equivalent

1. $\Delta(f) \neq 0$.
2. The polynomial f has no double zeroes in $\mathbb{C}$.
3. The decomposition of f in $\mathbb{Q}[X]$ has no multiple prime factors.
4. The polynomial f and its derivative f' are relatively prime in $\mathbb{Q}[X]$.
5. The polynomial $f \mod p$ and $f' \mod p$ are relatively prime in $\mathbb{F}_p[X]$ for almost all prime numbers p.

Proof. Let $f \in \mathbb{Z}[X]$ be monic and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ it roots in $\mathbb{C}$.
(1) $\Rightarrow$ (2). Suppose that $\alpha_i = \alpha_j$ for some $i \neq j$. Then

$$\Delta(f) = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j) = 0,$$

which is a contradiction. Therefore if f has non-zero discriminant it has no double zeroes in $\mathbb{C}$.
(2) $\Rightarrow$ (3).
(3) $\Rightarrow$ (4).
(4) $\Rightarrow$ (5). If f and f' are relatively prime in $\mathbb{Q}[X]$ then
(1) $\Rightarrow$ (1). □

Exercise 14.19
Let $f \in \mathbb{Q}[X]$ be a monic polynomial with $n = \deg(f)$ distinct complex roots. Prove: the sign of $\Delta(f)$ is equal to $(-1)^s$ where $2s$ is the number of non-real zeroes of f.

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be all the roots of f. Then each term $(\alpha_i - \alpha_j)^2$ in the discriminant falls into one of 3 cases

1. Both α_i and α_j are non-real. Then
   (a) If $\alpha_j = \overline{\alpha_i}$ then $\alpha_i - \alpha_j$ is purely complex and $(\alpha_i - \alpha_j)^2$ is negative.
   (b) If $\alpha_j \neq \overline{\alpha_i}$ then $\overline{\alpha_i}$ and $\overline{\alpha_j}$ are also roots of f and the term
   $$(\alpha_i - \alpha_j)^2(\overline{\alpha_i} - \overline{\alpha_j})^2 = \left((\overline{\alpha_i - \alpha_j})(\alpha_i - \alpha_j)\right)^2 = |\alpha_i - \alpha_j|^2$$
   is positive.
2. α_i is non-real and α_j is real. Then $\overline{\alpha_i}$ is a root of f and the term
   $$(\alpha_i - \alpha_j)^2(\overline{\alpha_i} - \alpha_j)^2 = |\alpha_i - \alpha_j|^2$$
   is positive.
3. Both α_i and α_j are real. Then $(\alpha_i - \alpha_j)^2$ is positive.

Since the only negative terms are of the form $(\alpha_i - \overline{\alpha_i})^2$ and there are $2s$ non-real roots the sign of the determinant is $(-1)^s$.

□

Exercise 14.20
Prove: $f(X) = X^3 + pX + q \in \mathbb{R}[X]$ has three (counted with multiplicity) real zeroes $\iff 4p^3 + 27q \leq 0$.

Proof. By Ex. 16 we know that $\Delta(f) = (-1)^3\left(3^3q^2 + 2^2p^3\right) = -27q^2 - 4p^3$. Let a, b and c be the roots of f. If $a, b, c \in \mathbb{R}$ then

$$-27q^2 - 4p^3 = \Delta(f) = (a-b)^2(a-c)^2(b-c)^2 \geq 0$$

and so $4p^3 + 27q \leq 0$.

Now suppose that $a = x + yi$ and $b = x - yi$ are complex conjugates and c is real. Then

$$\begin{aligned} -27q^2 - 4p^3 &= \Delta(f) \\ &= (a-b)^2(a-c)^2(b-c)^2 \\ &= -4y^2\left((a-c)(\overline{a-c})\right)^2 \\ &= -4y^2|a-c|^2 \\ &\leq 0. \end{aligned}$$

Hence $4p^3 + 27q \geq 0$ and the result follows by contraposition. □

Exercise 14.21
Express $p_4 = \sum_n T_1^4$ in elementary symmetric polynomials

Solution. Let $n \geq 4$. Starting with

$$\begin{aligned} s_1^4 &= \left(\sum_n T_1\right)^4 \\ &= \sum_n T_1^4 + 4\sum_n T_1^3 T_2 + 12\sum_n T_1^2 T_2 T_3 + 6\sum_n T_1^2 T_2^2 + 24\sum_n T_1 T_2 T_3 T_4. \end{aligned}$$

To understand how to coefficients of the sum are obtained, consider the number of ways the T_i can be arranged. For example, $T_1^4 = T_1T_1T_1T_1$ can only be arranged in 1 way but $T_1^2T_2T_3 = T_1T_1T_2T_3$ can be arrange in $\frac{4!}{2} = 12$ ways (where we divided by 2 since the two T_1 can be swapped in any given arrangement). Then

$$s_1^2 s_2 = \left(\sum_n T_1\right)^2 s_2 = \left(\sum_n T_1^2 + 2\sum_n T_1 T_2\right) s_2 = \sum_n T_1^3 T_2 + \sum_n T_1^2 T_2 T_3 + 2s_2^2.$$

So far we have

$$\begin{aligned} p_4 &= s_1^4 - 4\left(s_1^2 s_2 - 2s_2^2 - \sum_n T_1^2 T_2 T_3\right) - 12\sum_n T_1^2 T_2 T_3 - 6\sum_n T_1^2 T_2^2 - 24\sum_n T_1 T_2 T_3 T_4 \\ &= s_1^4 - 4s_1^2 s_2 + 8s_2^2 - 24s_4 - 6\sum_n T_1^2 T_2^2 - 8\sum_n T_1^2 T_2 T_3. \end{aligned}$$

So continuing with $\sum_n T_1^2 T_2^2$ we get

$$s_2^2 = \left(\sum_n T_1 T_2\right)^2 = \sum_n T_1^2 T_2^2 + 2\sum_n T_1^2 T_2 T_3 + 6\sum_n T_1 T_2 T_3 T_4.$$

Finding the coefficients here is slightly trickier since s_2 contains pairs not all arrangements are allowed. For example, $T_1^2T_2^2$ can only come from the pair T_1T_2. On the other hand $T_1T_2T_3T_4$ can come from T_1T_2 and T_3T_4 or T_1T_4 and T_2T_3 and so on. We choose the first pair ($\binom{4}{2} = 6$ ways) which also fixes the second pair and so there are 6 ways to get $T_1T_2T_3T_4$. Hence

$$\begin{aligned} p_4 &= s_1^4 - 4s_1^2 s_2 + 8s_2^2 - 24s_4 - 6\left(s_2^2 - 2\sum_n T_1^2 T_2 T_3 - 6s_4\right) - 8\sum_n T_1^2 T_2 T_3 \\ &= s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 12s_4 + 4\sum_n T_1^2 T_2 T_3. \end{aligned}$$

Using Exercise 14.10 we get

$$\begin{aligned} p_4 &= s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 12s_4 + 4(s_1 s_3 - 4s_4) \\ &= s_1^4 - 4s_1^2 s_2 + 2s_2^2 - 4s_4 + 4s_1 s_3 \end{aligned}$$

Exercise 14.22
A rational function $f \in \mathbb{Q}[T_1, \ldots, T_n]$ is called symmetric if it is invariant under all permutations of the variables T_i. Prove that every symmetric rational function is a rational function in the elementary symmetric functions.

Proof. Let $f \in \mathbb{Q}[T_1, \ldots, T_n]$ be a symmetric rational function. Then $f = g/h$ for g, h polynomials. If h is a symmetric polynomial then $g = fh$ is symmetric as well. By the fundamental theorem of symmetric polynomial both g and h can be written in terms of elementary symmetric polynomials and we're done. If h is not symmetric, then let

$$\tilde{h} = \prod_{\sigma \in S_n \setminus \{e\}} \sigma(h)$$

and then $h\tilde{h}$ is symmetric so $f = \frac{g\tilde{h}}{h\tilde{h}}$ which is again the case above. □

Exercise 14.23
Write $\sum_n T_1^{-1}$ and $\sum_n T_1^{-2}$ as rational functions in $\mathbb{Q}[s_1, \ldots, s_n]$

Solution. Starting with

$$\sum_n T_1^{-1} = \frac{1}{T_1} + \cdots + \frac{1}{T_n}.$$

We multiply by $1 = \frac{s_n}{s_n}$ and simplify

$$\begin{aligned} \frac{s_n}{s_n} \sum_n T_1^{-1} &= \frac{T_1 T_2 \cdots T_n}{T_1 T_2 \cdots T_n} \left(\frac{1}{T_1} + \cdots + \frac{1}{T_n} \right) \\ &= \frac{s_{n-1}}{s_n} \end{aligned}$$

For the second expression we present to approaches.

1. Observing that

$$\left(\sum_n T_1^{-1} \right)^2 = \sum_n T_1^{-2} + 2 \sum_n T_1^{-1} T_2^{-1}$$

we can write using the previous part

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2}{s_n^2} - 2 \sum_n T_1^{-1} T_2^{-1}$$

and multiplying by the second term by $\frac{s_n}{s_n}$ we get

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2}{s_n^2} - 2 \left(\frac{1}{T_1 T_2} + \cdots + \frac{1}{T_{n-1} T_n} \right) \frac{T_1 \cdots T_n}{T_1 \cdots T_n} = \frac{s_{n-1}^2}{s_n^2} - 2 \frac{s_{n-2}}{s_n}.$$

Hence $\sum_n T_1^{-2} = \frac{s_{n-1}^2 - 2 s_{n-2} s_n}{s_n^2}$.

2. The second approach is slightly more involved. We start by multiplying by 1 in a clever (but different) way

$$\left(\sum_n T_1^{-2}\right)\frac{s_n^2}{s_n^2} = \left(\frac{1}{T_1^2}+\cdots+\frac{1}{T_n^2}\right)\frac{T_1^2\cdots T_n^2}{T_1^2\cdots T_n^2} = \frac{\sum_n T_1^2\cdots T_{n-1}^2}{s_n^2}.$$

Then $\sum_n T_1^2\cdots T_{n-1}^2$ is obviously (condescending much?) a symmetric polynomial and so we can use our trusty algorithm. Starting with

$$\begin{aligned} s_1^{2-2}s_2^{2-2}\cdots s_{n-1}^{2-0} &= s_{n-1}^2 \\ &= \left(\sum_n T_1\cdots T_{n-1}\right)^2 \\ &= \sum_n T_1^2\cdots T_{n-1}^2 + 2\sum_n T_1^2\cdots T_{n-2}^2 T_{n-1}T_n. \end{aligned}$$

Moving to the second term

$$\begin{aligned} s_1^{2-2}\cdots s_{n-2}^{2-1}s_{n-1}^{1-1}s_n^1 &= s_{n-2}s_n \\ &= \left(\sum_n T_1\cdots T_{n-2}\right)T_1\cdots T_n \\ &= \sum_n T_1^2\cdots T_{n-2}^2 T_{n-1}T_n \end{aligned}$$

and it follows that

$$\sum_n T_1^2\cdots T_{n-1}^2 = s_{n-1}^2 - 2s_{n-2}s_n.$$

So we conclude that

$$\sum_n T_1^{-2} = \frac{s_{n-1}^2 - 2s_{n-2}s_n}{s_n^2}$$

which is reassuring.

Note that in the first approach we stumbled upon something rather interesting:

$$\sum_n T_1^{-1}\cdots T_k^{-1} = \frac{s_{n-k}}{s_n}$$

the proof of which is left as an exercise to the reader.

Exercise 14.24

Field Extensions

Exercise 21.18
Let $K \subset L$ be an algebraic extension. For $\alpha, \beta \in L$ prove that we have

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K] .$$

Show that equality does not always hold. Does equality always hold if $[K(\alpha) : K]$ and $[K(\beta) : K]$ are relatively prime?

Proof. Let f and g be the minimal polynomials of α and β (respectively) in $K[x]$ and f' be the minimal polynomial of α in $K(\beta)[x]$. If $\deg f' > \deg f$ then f is a lower degree polynomial in $K(\beta)[x]$ with $f(\alpha) = 0$ which is a contradiction. Hence $\deg f' \leq \deg f$ and so

$$\begin{aligned}
[K(\alpha, \beta) : K] &= [K(\alpha, \beta) : K(\beta)] \cdot [K(\beta) : K] \\
&= \deg f' \cdot \deg g \\
&\leq \deg f \cdot \deg g \\
&= [K(\alpha) : K] \cdot [K(\beta) : K] ,
\end{aligned}$$

as desired.

To show that equality does not always hold consider $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ but

$$[\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) : \mathbb{Q}] = 4 \cdot [\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 4 < 8$$

since $\left(\sqrt[4]{2}\right)^2 = \sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$

Lastly, suppose that $\deg f$ and $\deg g$ are relatively prime. Since

$$\begin{aligned}
[K(\alpha, \beta) : K] &= [K(\alpha, \beta), K(\alpha)] \cdot \deg f \\
&= [K(\alpha, \beta), K(\beta)] \cdot \deg g
\end{aligned}$$

it follows that $[K(\alpha, \beta) : K]$ is divisible by $\deg f$ and $\deg g$ and since they are relatively prime it is also divisible by $\deg f \cdot \deg g$. But we know that $[K(\alpha, \beta) : K] \leq \deg f \cdot \deg g$ and so $[K(\alpha, \beta) : K] = \deg f \cdot \deg g$. □

Exercise 21.19
Let $K \subset K(\alpha)$ be an extension of odd degree. Prove that $K(\alpha^2) = K(\alpha)$.

Proof. Let f be the minimal polynomial of α in $K[x]$. Then $\deg f = 2n + 1$ for some $n \in \mathbb{Z}_+$. Since $\alpha^2 \in K(\alpha)$ we get the tower $K(\alpha)/K\left(\alpha^2\right)/K$ and so

$$[K(\alpha) : K] = \left[K(\alpha) : K\left(\alpha^2\right)\right] \cdot \left[K\left(\alpha^2\right) : K\right] .$$

Let g be the minimal polynomial of α in $K\left(\alpha^2\right)$. Then $\deg g \leq 2$ since $x^2 - \alpha^2 \in K\left(\alpha^2\right)$ is a polynomial with a root α. Since $[K(\alpha) : K]$ is odd, it is not divisible by two and so $\deg g = 1$. Hence $\left[K(\alpha) : K\left(\alpha^2\right)\right] = 1$ and it follows that $K(\alpha) = K\left(\alpha^2\right)$. □

Exercise 21.23
Show that every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}\left(\sqrt{d}\right)$ with $d \in \mathbb{Z}$. For what d do we obtain the cyclotomic field $\mathbb{Q}(\zeta_3)$?

Proof. Let $K/\mathbb{Q}$ be a quadratic extension. Take $\alpha \in K \setminus \mathbb{Q}$. Then

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$$

and so

$$2 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \, [\mathbb{Q}(\alpha) : \mathbb{Q}] \, .$$

If $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$ then $\mathbb{Q}(\alpha) = \mathbb{Q}$ and so $\alpha \in \mathbb{Q}$, which contradicts our assumption. It follows that $[K : \mathbb{Q}(\alpha)] = 1$ and so $K = \mathbb{Q}(\alpha)$. Let

$$f(x) = x^2 + a_1 x + a_0 \in \mathbb{Q}[x]$$

be the minimal polynomial of α. Let $d = \frac{a_1^2}{4} - a_0 \in \mathbb{Q}$ and note that $a_0 = -\alpha a_1 - \alpha^2$. Then

$$\begin{aligned} \sqrt{d} &= \sqrt{\frac{a_1^2}{4} - a_0} \\ &= \sqrt{\frac{a_1^2}{4} + a_1\alpha + \alpha^2} \\ &= \frac{a_1 + 2\alpha}{2}. \end{aligned}$$

Hence $\sqrt{d} \in \mathbb{Q}(\alpha)$. By similar calculations we get $\alpha = \frac{2\sqrt{d} - a_1}{2} \in \mathbb{Q}(\sqrt{d})$. Hence $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. Of course, it is not yet the case the d is an integer. Suppose that $d = \frac{p}{q}$. Since $\sqrt{d} = \frac{1}{q^2}\sqrt{qp} \in \mathbb{Q}(\sqrt{qp})$ we have

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{qp})$$

with $qp \in \mathbb{Z}$ as desired. □

Exercise 21.24
Is every cubic extension of $\mathbb{Q}$ of the form $\mathbb{Q}\left(\sqrt[3]{d}\right)$ for some $d \in \mathbb{Q}$?

Solution. No. Let α be a root of the monic irreducible polynomial $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ (possible roots are ± 1 and they both clearly don't work). There are three choices for α all in $\mathbb{R}$ (why? Using Exercise 14.16 the determinant is $4 \cdot (-3)^3 + 27 \cdot 1 = -81 < 0$ and so by Exercise 14.20 f has three real roots). Therefore there are three embeddings $\varphi : \mathbb{Q}(\alpha) \to \mathbb{C}$ and $\operatorname{Im} \varphi \subset \mathbb{R}$.

Assume for contradiction that there exists an isomorphism $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\sqrt[3]{d})$ for some $d \in \mathbb{Q}$. Since $\sqrt[3]{d} \notin \mathbb{Q}$, $x^3 - d$ is irreducible and so $f_{\mathbb{Q}}^{\sqrt[3]{d}} = x^3 - d$. Since $f_{\mathbb{Q}}^{\sqrt[3]{d}}$ has one real and two non-real roots (again, using exercises 14.16 and

14.20 with the fact that $27 \cdot (-d)^2 > 0$) there are three embeddings of $\mathbb{Q}(\sqrt[3]{d})$ into $\mathbb{C}$ to of which are not subsets of $\mathbb{R}$.

Let $\Phi : \mathbb{Q}(\sqrt[3]{d}) \to \mathbb{C}$ be one of the latter. Then $\Phi \circ \phi : \mathbb{Q}(\alpha) \to \mathbb{C}$ is an imbedding of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ whose image is not a subset of $\mathbb{R}$. Therefore we conclude that ϕ doesn't exists.

Exercise 21.26
Let $M = \mathbb{Q}(\alpha) = \mathbb{Q}(1 + \sqrt{2} + \sqrt{3})$. Show that M is of degree 4 over $\mathbb{Q}$, determine the minimal polynomial and write $\sqrt{2}$ and $\sqrt{3}$ in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$. Also prove that the group $G = \mathrm{Aut}_{\mathbb{Q}}(M)$ is isomorphic to V_4 and that $f_{\mathbb{Q}}^{\alpha} = \prod_{\sigma \in G} X - \sigma(\alpha) \in \mathbb{Q}[X]$.

Solution. Let $\beta = \alpha - 1 = \sqrt{2} + \sqrt{3}$. Then clearly $M = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Let

$$\begin{aligned} f(x) &= (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \\ &= x^4 - 10x^2 + 1 \in \mathbb{Q}[x] \end{aligned}$$

and so $f(\beta) = 0$ by construction.

Is f the minimal polynomial of β in $\mathbb{Q}[x]$? It is if we can prove that $[M : \mathbb{Q}] = 4$. From

$$(\sqrt{2} + \sqrt{3})(\sqrt{3} - \sqrt{2}) = 1$$

It follows that $\beta^{-1} = \sqrt{3} - \sqrt{2}$. Therefore

$$\sqrt{2} = \frac{1}{2}(\beta - \beta^{-1}) \quad \text{and} \quad \sqrt{3} = \frac{1}{2}(\beta + \beta^{-1})$$

and so $M = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence we have the towers $M/\mathbb{Q}(\sqrt{2})/Q$ and $M/\mathbb{Q}(\sqrt{3})/Q$. Let $g(x) = x^2 - 3$. Suppose it is not the minimal polynomial of $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$. Then there exists $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ such that

$$0 = g(a + b\sqrt{2}) = a^2 + 2b^2 - 3 + 2ab\sqrt{2}.$$

But since

$$\begin{cases} a^2 + 2b^2 - 3 = 0 \\ 2ab = 0 \end{cases}$$

has no solutions it follows that no such element exists. Therefore g is the minimal polynomial of $\sqrt{3}$ and $[M : \mathbb{Q}(\sqrt{2})] = \deg g = 2$. Since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ in $\mathbb{Q}$ we conclude that

$$[M : \mathbb{Q}] = [M : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q})] = 4$$

and therefore f is the minimal polynomial of β.

Thus $f(x-1)$ is the minimal polynomial of α in $\mathbb{Q}$. From $f(\beta) = 0$ it follows that $1 = \beta(10\beta - \beta^3)$ and so $\beta^{-1} = 10\beta - \beta^3$. Hence

$$\sqrt{2} = \frac{1}{2}\left(\beta - \beta^{-1}\right) = \frac{1}{2}\left(\beta - 10\beta + \beta^3\right) = \frac{1}{2}\left(-9(\alpha - 1) + (\alpha - 1)^3\right)$$

and

$$\sqrt{3} = \frac{1}{2}\left(\beta + \beta^{-1}\right) = \frac{1}{2}\left(11(\alpha-1) - (\alpha-1)^3\right)$$

Let $G = \mathrm{Aut}(M)$ and take $\sigma \in G$. Then by definition $\sigma(1) = 1$ and it follows by induction and the properties of isomorphism that $\sigma(a) = a$ for all $a \in \mathbb{Z}$. Since $1 = \sigma(1) = \sigma(a \cdot a^{-1}) = \sigma(a) \cdot \sigma(a)^{-1} = a \cdot a^{-1}$ it also follows that $\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$. Hence σ restricted to $\mathbb{Q}$ is simply the identity map. Therefore σ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Since $0 = \sigma(0) = \sigma(\sqrt{2}^2 - 2) = \sigma(\sqrt{2})^2 - 2$ the only options are $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Similarly we conclude that $\sigma(\sqrt{3}) = \pm\sqrt{3}$. This gives four possible automorphism. Take $\sigma, \tau \in G$ such that $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(x) = x\ \forall x \in M \setminus \{\sqrt{2}\}$ and $\tau(\sqrt{3}) = -\sqrt{3}, \tau(x) = x$ $\forall x \in M \setminus \{\sqrt{3}\}$. Since

$$\sigma \circ \sigma = \tau \circ \tau = \sigma \circ \tau \circ \sigma \circ \tau = e$$

where e is the identity map it follows that G is isomorphic to V_4, the Klein four-group.

Lastly, consider

$$\begin{aligned}\tilde{f} &= \prod_{\sigma \in G} x - \sigma(\alpha) \\ &= (x - 1 - \sqrt{2} - \sqrt{3})(x - 1 + \sqrt{2} - \sqrt{3})(x - 1 - \sqrt{2} + \sqrt{3}) \\ &\qquad (x - 1 + \sqrt{2} + \sqrt{3}).\end{aligned}$$

Hence $\tilde{f}(x) = f(x-1)$ which we already proved is the minimal polynomial of α in $\mathbb{Q}[x]$.

Exercise 21.28
Prove $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}\sqrt[3]{3}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$. Determine the minimum polynomials of $\sqrt{2}\sqrt[3]{3}$ and $\sqrt{2} + \sqrt[3]{3}$ over $\mathbb{Q}$.

Proof. Clearly we have that $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ and $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Since $x^2 - 2$ is irreducible (Eisenstein with $p = 2$) and $x^3 - 3$ is irreducible (Eisenstein with $p = 3$) and $(3, 2) = 1$ it follows that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 6$.

Now consider $f(x) = x^6 - 72$. Then $f(\sqrt{2}\sqrt[3]{3}) = 0$ and so $[\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) : \mathbb{Q}] \leq 6$. Suppose that $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ for $a(x), b(x)$ non constant. Furthermore suppose without loss of generality that $\deg a \geq \deg b$. Reducing f modulo 7 we find that

$$\overline{f}(x) = x^6 - 2 = x^6 - 9 = (x^3 - 3)(x^3 + 3) = \overline{a}(x)\overline{b}(x) \in \mathbb{F}_7[x]$$

Reducing f modulo 5 we get

$$\overline{f}(x) = x^6 - 2 = x^6 + 8 = (x^4 - 2x^2 + 4)(x^2 + 2) = \overline{a}(x)\overline{b}(x) \in \mathbb{F}_5[x].$$

Since f modulo 5 has no cubic terms it follows that $\deg a = 6$ and $\deg b = 1$ and so f is irreducible. Therefore $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = \deg f = 6$ and since $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ it follows that $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.

Let $\alpha = \sqrt{2}, \beta = \sqrt[3]{3}$ and $\gamma = \alpha + \beta$. Let $L = \mathbb{Q}(\alpha, \beta)$, $K = \mathbb{Q}(\gamma)$ and suppose that $\alpha, \beta \notin K$. Since if one of α, β is in K, we get the other one for free it follows that $L = K(\alpha) = K(\beta)$. Then the minimal polynomial of α in $K[X]$ is of degree 2 since α is a root of $X^2 - 2$ and we assumed $\alpha \notin K$. Since $X^3 - 3$ has one real root and two non-real roots it follows that it is the minimal polynomial of β in $K[X]$. Hence we conclude

$$2 = [K(\alpha) : K] = [L : K] = [K(\beta) : K] = 3,$$

clearly a contradiction. Therefore $K = L$ and so $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. □

Exercise 21.29
Take $K = \mathbb{Q}(\alpha)$ with $f_{\mathbb{Q}}^{\alpha} = x^3 + 2x^2 + 1$.

1. Determine the inverse of $\alpha + 1$ in the basis $\{1, \alpha, \alpha^2\}$ of K over $\mathbb{Q}$.
2. Determine the minimal polynomial of α^2 over $\mathbb{Q}$.

Solution.

1. Since

$$\begin{aligned} 0 &= \alpha^3 + 2\alpha^2 + 1 \\ &= (\alpha + 1)(\alpha^2 + \alpha - 1) + 2. \end{aligned}$$

   It follows that $(\alpha + 1)^{-1} = -\frac{1}{2}(\alpha^2 + \alpha - 1)$.

2. From $\alpha^3 + 2\alpha^2 + 1 = 0$ it follows that $\alpha^3 = -2\alpha^2 - 1$. Squaring both sides we get that $\alpha^6 = 4\alpha^4 + 4\alpha^2 + 1$ or alternatively

$$\left(\alpha^2\right)^3 - 4\left(\alpha^2\right)^2 - 4\left(\alpha^2\right) - 1 = 0.$$

   By Ex. 19 we know that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$. Therefore the minimal polynomial of α^2 over $\mathbb{Q}$ has degree 3 and it follows that

$$f_{\mathbb{Q}}^{\alpha^2}(x) = x^3 - 4x^2 - 4x - 1.$$

Exercise 21.30
Define the cyclotomic field $\mathbb{Q}(\zeta_5)$ and let $\alpha = \zeta_5^2 + \zeta_5^3$.

1. Show that $\mathbb{Q}(\alpha)$ is a quadratic extension of $\mathbb{Q}$ and determine $f_{\mathbb{Q}}^{\alpha}$.
2. Prove: $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$
3. Prove: $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ and $\sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{8}}$

Proof.

1. The degree of the 5th cyclotomic polynomial

$$\Phi_5(x) = \prod_{\substack{1\le k\le 5\\(k,5)=1}} \left(x - e^{\frac{2\pi k}{5}i}\right) = x^4 + x^3 + x^2 + x + 1$$

is 4 and since $\Phi_5 = f_{\mathbb{Q}}^{\zeta_5}$ it follows that $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Thus

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] \mid 4.$$

Note that $\zeta_5^3 = \frac{1}{\zeta_5^2} = \overline{\zeta_5^2}$. Hence $\alpha = \zeta_5^2 + \zeta_5^3 = \zeta_5^2 + \overline{\zeta_5^2} \in \mathbb{R}$ and so $\mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\zeta_5)$. Together with the fact that ζ_5 is a root of $x^3+x^2-\alpha \in \mathbb{Q}(\alpha)$ it follows that

$$1 < [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] \le 3 \implies [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)] = 2.$$

Finally, since $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\alpha)/\mathbb{Q}$ is a tower of fields and

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_5) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\alpha)]} = 2$$

it follows that $\mathbb{Q}(\alpha)$ is a quadratic extension.

Let $w = \zeta_5^2$. Then $\alpha = w + \frac{1}{w}$ and $\Phi_5(w) = 0$ by definition of Φ_5. Since $w \neq 0$ it follows that

$$\begin{aligned}
0 &= 1 + w + w^2 + w^3 + w^4 \\
0 &= \frac{1}{w^2} + \frac{1}{w} + 1 + w + w^2 \\
0 &= \left(w + \frac{1}{w}\right)^2 + w + \frac{1}{w} - 1 \\
0 &= \alpha^2 + \alpha - 1.
\end{aligned}$$

Since $x^2 + x - 1$ is monic polynomial of degree 2 we conclude that $f_{\mathbb{Q}}^{\alpha} = x^2 + x - 1$.

2. By construction α is a root of $x^2 + x - 1$ and so

$$\alpha \in \left\{ \frac{-1 \pm \sqrt{5}}{2} \right\}.$$

Since we can write α as polynomial in $\sqrt{5}$ and vice versa it follows that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

3. Let $\zeta_5 = e^{\frac{6\pi}{5}i}$. Then $w = \zeta_5^2 = e^{\frac{2\pi}{5}i}$ and

$$\cos\frac{2\pi}{5} = \frac{w + \overline{w}}{2} = \frac{\alpha}{2}.$$

Thus $2\cos\frac{2\pi}{5}$ is a root of f_Q^α. Since $\frac{2\pi}{5}$ is in the first quadrant, $\cos\frac{2\pi}{5}$ is positive and so

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

Therefore we also have

$$\begin{aligned}\sin\frac{2\pi}{5} &= \sqrt{1-\cos^2\frac{2\pi}{5}} \\ &= \sqrt{\frac{5+\sqrt{5}}{8}}.\end{aligned}$$

□

Exercise 21.31
Let $\overline{K}$ be an algebraic closure of K and $L \subset \overline{K}$ a field that contains K. Prove that $\overline{K}$ is an algebraic closure of L.

Proof. Let $\overline{L} = \{\alpha \in \overline{K} \mid \alpha \text{ algebraic over } \}$ be the algebraic closure of L. By definition we have that $\overline{L} \subset \overline{K}$ so it is left to show the other inclusion. Let $\alpha \in \overline{K}$. Then α is algebraic over K by definition, and so there exists $f \in K[x]$ such that $f(\alpha) = 0$. Then $f \in L[x]$ since $K \subset L$ and so α is algebraic over L. Therefore $\alpha \in \overline{L}$ and so $\overline{L} = \overline{K}$. □

Exercise 21.32
Let $K \subset L$ be a field extension and $\overline{K}$ the algebraic closure of K in L. Prove that every $\alpha \in L \setminus \overline{K}$ is transcendental over $\overline{K}$.

Proof. Suppose there exists $\alpha \in L \setminus \overline{K}$ that is algebraic over $\overline{K}$. Let

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

be the minimal polynomial of α in $\overline{K}[x]$. Let

$$K_1 = K(a_0, \ldots, a_{n-1}) \quad \text{and} \quad K_2 = K_1(\alpha).$$

Then K_1/K is an algebraic extension since $a_0, \ldots, a_n \in \overline{K}$ and K_2/K_1 is algebraic since $f \in K_1[x]$. So we have the tower of fields $K_2/K_1/K$ and it follows that K_2/K is an algebraic extension and so α is algebraic over K. By definition of algebraic closure, $\alpha \in \overline{K}$ which contradicts our assumption. Therefore α must be transcendental over $\overline{K}$. □

Exercise 21.35
Let $f \in K[x]$ be a polynomial of degree $n \geq 1$. Prove: $[\Omega_K^f : K]$ divides $n!$.

Proof. If $n = 1$, the K is splitting field of f and $[K : K] = 1$ divides $n! = 1$. Suppose the statement holds for some $n \geq 1$. There are two cases

1. Suppose f is irreducible, $\deg f = n+1$ and α is a root of f. Then $K(\alpha)$ is an extension of degree $n+1$ and $f(x) = (x-\alpha)g(x) \in K(\alpha)[x]$. Let M be the splitting field of g over $K(\alpha)$. Then $[M : K(\alpha)]$ divides $n!$ by the induction hypothesis. But M is also the splitting field of f over K and so

$$[M : K] = [M : K(\alpha)][K(\alpha) : K] = [M : K(\alpha)](n+1)$$

which divides $(n+1)!$.

2. Suppose f is a reducible polynomial of degree $n+1$. Let $f(x) = h(x)g(x)$ with h irreducible. Construct the tower of fields $M/L/K$ such that L is the splitting field of h over K and M is the splitting field of g over L. Then $[L : K]$ divides $(\deg h)!$ and $[M : L]$ divides $(\deg g)!$ by induction hypothesis. Hence

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

divides $(\deg h)! \cdot (\deg g)!$. And since

$$\binom{n+1}{\deg h} = \frac{(n+1)!}{(\deg h)!(n+1-\deg h)!} = \frac{(n+1)!}{(\deg h)!(\deg g)!}$$

is an integer it follows that $[M : K]$ divides $(n+1)!$.

□

Exercise 21.36
Let $d \in \mathbb{Z}$ be an integer that is not a third power in $\mathbb{Z}$. Prove that the splitting field $\Omega_{\mathbb{Q}}^{x^3-d}$ has degree 6 over $\mathbb{Q}$. What is the degree if d is a third power?

Proof. Let $f(x) = x^3 - d$. Suppose f has a root in $r/s \in \mathbb{Q}$. Then $s \mid 1$ and $r \mid d$ so $f(r) = r^3 - d = 0 \implies d = r^3$ which contradicts our assumption. Therefore $f(x)$ has no roots in $\mathbb{Q}$ and since $\deg f = 3$ it follows that f is irreducible. Then $\mathbb{Q}[X]/(f)$ is a field and $\alpha \equiv x \mod \left(x^3 - d\right)$ is a zero of f. Therefore f splits in $\mathbb{Q}(\alpha)$ as

$$x^3 - d = (x-\alpha)(x^2 + \alpha x + \alpha^2)$$

and

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

. Let $h(x) = x^2 + x + 1$. Then $h(x+1) = x^2 + 3x + 3$ is irreducible in $\mathbb{Q}[x]$ (Eisenstein with $p = 3$) and so $h(x)$ is irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]/(h)$ is a quadratic extension, it cannot be a subfield of the cubic extension $\mathbb{Q}[x]/(f)$ and so $h(x)$ has no zeros in $\mathbb{Q}(a)$. Hence it is irreducible in $\mathbb{Q}(a)[x]$. It follows that $\mathbb{Q}(\alpha)[x]/(h) \cong \mathbb{Q}(\alpha)(\beta)$ is a quadratic extension for $\beta \equiv x \mod \left(x^2 + x + 1\right)$. Then

$$f(x) = (x-\alpha)(x-\alpha\beta)(x+\alpha\beta+\alpha)$$

and so $\mathbb{Q}(\alpha, \beta)$ is the splitting of f. Moreover

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$$

as desired.

If $d = r^3$ for some $r \in \mathbb{Z}$ then $f(x)$ is reducible since

$$f(x) = (x - r)(x^2 + rx + r^2) \in \mathbb{Q}[x].$$

Then $r\beta$ is a root of $X^2 + rx + r^2$ and so the quadratic extension $\mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^2 + x + 1)$ is the splitting field of f. □

Exercise 21.37
Determine the degree of the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

Solution. Since

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i),$$

the splitting field of $x^4 - 2$ is $\mathbb{Q}(\sqrt{2}, i)$. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Therefore the degree of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}(\sqrt{2})$ is less than 2. It can't be 1 since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $i \notin \mathbb{R}$ and so $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. Therefore

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

Exercise 21.38
Determine the degree of the splitting field of $x^4 - 4$ and $x^4 + 4$. Explain why the notation $\mathbb{Q}(\sqrt[4]{4})$ and $\mathbb{Q}(\sqrt[4]{-4})$ is not used for the fields obtained through the adjunction of a zero of, respectively, $x^4 - 4$ and $x^4 + 4$ to $\mathbb{Q}$.

Solution. Note that

$$x^4 - 4 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)\left(x + \sqrt{2}i\right)\left(x - \sqrt{2}i\right).$$

Since $i = \left(\sqrt{2}\right)^{-1}\sqrt{2}i$ the splitting field of $x^4 - 4$ is $\mathbb{Q}\left(\sqrt{2}, \sqrt{2}i\right) = \mathbb{Q}\left(\sqrt{2}, i\right)$. Similarly

$$x^4 + 4 = (x - 1 - i)(x - 1 + i)(x + 1 - i)(x + 1 + i),$$

and so the splitting filed of $x^4 + 4$ is $\mathbb{Q}(i)$. To compute the degree of the splitting fields note that:

1. $(x + 1)^2 + 1$ is irreducible in $\mathbb{Q}[x]$ (Eisenstein with $p = 2$) hence $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ and so $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$.
2. $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ (Eisenstein with $p = 2$)
3. $\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \leq 2$ since the minimal polynomial of i over $\mathbb{Q}$ is of degree two by (1). However $\mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{R}$ and $i \notin \mathbb{R}$ so the degree cannot be one. Therefore $\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$.

It follows that

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2$$

and

$$\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 4.$$

Outside the fact that the notation $\mathbb{Q}\left(\sqrt[4]{-4}\right)$ is ambiguous (which of the four roots does it stand for?), it is also misleading. It might seem like an extension of degree four, but as shown above it is of degree 2, regardless of which of the roots you assign to $\sqrt[4]{-4}$. Similarly the degree of $\mathbb{Q}\left(\sqrt[4]{4}\right)$ is two and not four since $\sqrt[4]{4} = \sqrt{2}$. Therefore it is clearer and to simply write $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(1+i)$ for the adjunction of a zero of, respectively, $x^4 - 4$ and $x^4 + 4$ to $\mathbb{Q}$.

Finite Fields

Exercise 22.4
Let $f \in \mathbb{F}_q[x]$ ($q = p^n$) be monic irreducible polynomial of degree d. Then every zero α of f in $\overline{\mathbb{F}_p}$ satisfies the equality

$$f = \prod_{i=0}^{d-1} \left(x - \alpha^{q^i}\right) \in \overline{F_p}[x]$$

Proof. Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree d and $\alpha \in \overline{\mathbb{F}_p}$ a root of f. Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be given by $F(x) = x^q$ which is an automorphism on $\mathbb{F}_q(\alpha)$. Then F^d is the identity and so $|F| \leq d$. Suppose $|F| = k \mid d$. Then $a^{q^k} = a$ for all $a \in \mathbb{F}_q(\alpha)$, but $x^{q^k} - x$ has only q^k roots while $\mathbb{F}_q(\alpha)$ has q^d elements. Therefore the order of F in $\mathrm{Aut}(\mathbb{F}_q(\alpha))$ is d.

Suppose $f(x) = \sum_{i=0}^{d} a_i x^i$. Then for any $\sigma \in \mathrm{Aut}(\mathbb{F}_q(\alpha))$

$$0 = \sigma(0) = \sigma(f(\alpha)) = \sum_{i=0}^{d} \sigma(a_i \alpha^i) = \sum_{i=0}^{d} a_i \sigma(\alpha)^i$$

since $\sigma(a) = a^q = a$ for all $a \in \mathbb{F}_q$. Therefore $\sigma(\alpha)$ is a root of f for any $\sigma \in \mathrm{Aut}(\mathbb{F}_q(\alpha))$. Since the map $\mathrm{Aut}(\mathbb{F}_q(\alpha)) \to \{\alpha \in \overline{\mathbb{F}_p} \mid f(\alpha) = 0\}$ taking σ to $\sigma(\alpha)$ is injective, it follows that $|\mathrm{Aut}(\mathbb{F}_q(\alpha))| \leq d$. Therefore $\mathrm{Aut}(\mathbb{F}_q(\alpha)) = d$ and so the group of automorphism on $\mathbb{F}_q(\alpha)$ is generated by F. Therefore it follows that

$$f = \prod_{\sigma \in \mathrm{Aut}(\mathbb{F}_q(\alpha))} (x - \sigma(\alpha)) = \prod_{i=0}^{d-1} \left(x - \alpha^{q^i}\right) \in \overline{F_p}[x]$$

for any root α of f. □

Exercise 22.6
Give an explicit isomorphism $\mathbb{F}_5[x]/(x^2 + x + 1) \xrightarrow{\sim} \mathbb{F}_5(\sqrt{2})$

Solution. Let $\varphi : \mathbb{F}_5[x]/(x^2+x+1) \xrightarrow{\mathbb{F}}_5 (\sqrt{2})$ be an isomorphism and α the equivalence class of x in $\mathbb{F}_5[x]/(x^2+x+1)$. Since φ is identity on $\mathbb{F}_5$, we only need to find where α is mapped to. Suppose

$$\varphi(\alpha) = c + d\sqrt{2}.$$

Then $\left(c+d\sqrt{2}\right)^2 + c + d\sqrt{2} + 1 = 0$. Hence

$$\begin{cases} d(2c+1) = 0 \\ c^2 + 2d^2 + c + 1 = 0 \end{cases}.$$

Since $d = 0$ would be a contradiction it follows from the first equation that $c = 2$. Substituting into the second we get $4 + 2d^2 + 3 = 2d^2 + 2$ and so $2d^2 = 3$. Therefore $d = 2, 3$ and either value will give us an isomorphism. So let

$$\varphi(a + b\alpha) = a + b(2 + 2\sqrt{2}) = 2a + 2b\sqrt{2}.$$

Exercise 22.7
Show that $f(x) = x^2 + 2x + 2$ and $g = x^2 + x + 3$ are irreducible in $\mathbb{F}_7[x]$ and give an explicit isomorphism $\mathbb{F}_7[x]/(f) \xrightarrow{\sim} \mathbb{F}_7[x]/(g)$.

Solution. Check that every element of $\mathbb{F}_7$ is not a root.

We need to find $c + d\beta \in \mathbb{F}_7[x]/(g)$ such that

$$(c+d\beta)^2 + 2(c+d\beta) + 2 = 0.$$

Using that $\beta^2 = 6\beta + 4$ we get

$$\begin{aligned} 0 &= c^2 + 2cd\beta + d^2\beta^2 + 2c + 2d\beta + 2 \\ &= (2cd + 6d^2 + 2d)\beta + (c^2 + 4d^2 + 2c + 2). \end{aligned}$$

which is equivalent to

$$\begin{cases} d(2c + 6d + 2) = 0 \\ c^2 + 4d^2 + 2c + 2 = 0 \end{cases}.$$

Since $d \neq 0$ it follows that $c = 4d + 6$. Hence $d^2 = 1$ and so $d = 1, 6$. So $c = 3, 2$ and either pair would give us an isomorphism.

Exercise 22.8
Calculate the orders $1 - \sqrt{2}, 2 - \sqrt{2}$ and $3 - \sqrt{2}$ in $\mathbb{F}_5(\sqrt{2})^2$.

Solution. Note that $(1-\sqrt{2})^3 = 2$ and the order of 2 is 4. Hence the order of $(1-\sqrt{2})$ divides 12. Since $(1-\sqrt{2})^2 = 3 - 2\sqrt{2}, (1-\sqrt{2})^3 = 2, (1-\sqrt{2})^4 = 4$ and $(1-\sqrt{2})^6 = (1-\sqrt{2})^2(1-\sqrt{2})^4 = 8 = 3$ it follows that the order of $1-\sqrt{2}$ in $\mathbb{F}_5(\sqrt{2})$ is 12.

Exercise 22.11
Let p be a prime. Show that $\mathbb{F}_p(x)/(x^2+x+1)$ is a field if and only if $p \equiv 2 \mod 3$.

Proof. ($\Rightarrow$) Suppose $\mathbb{F}_p(x)/(x^2+x+1)$ is a field. So $f(x) = x^2+x+1$ is irreducible in $\mathbb{F}_p[x]$. Therefore $\mathbb{F}_p$ does not contain a non-trivial cube root of unity and so 3 doesn't divide $\left|\mathbb{F}_p^*\right| = p-1$. Since $f(x) = (x+2)^2$ in $\mathbb{F}_3[x]$ it can't be the case that p is congruent to 0 mod 3 and so $p \equiv 2 \mod 3$.

($\Leftarrow$) Suppose $\mathbb{F}_p(x)/(x^2+x+1)$ is not a field. Then $f(x) = x^2+x+1$ is reducible in $\mathbb{F}_p[x]$ and so f has a root $\alpha \in \mathbb{F}_p$. Then $\alpha \neq 0$ and $\alpha^3 = 1$. Therefore 3 divides $\left|\mathbb{F}_p^*\right| = p-1$ and so $p \equiv 1 \mod 3$.

□

Exercise 22.12
Let q be a prime power.

1. For what q is the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$ of the form $\mathbb{F}_q(\sqrt{x})$ with $x \in \mathbb{F}_q$?
2. For what q is the cubic extension $\mathbb{F}_{q^3}$ of $\mathbb{F}_q$ of the form $\mathbb{F}_q(\sqrt[3]{x})$ with $x \in \mathbb{F}_q$?

Solution.

1. Let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ be given by $\varphi(a) = a^2$. If $q = p^n$ is even, then $p = 2$ and φ is a field isomorphism. Therefore $\mathbb{F}_q(\sqrt{b}) = \mathbb{F}_q$ for all $x \in \mathbb{F}_q$. If q is odd, then $(-1)^2 = 1 = 1^2$ so the map is not injective and so it's not surjective. Therefore there exists $b \in \mathbb{F}_q$ such that $\sqrt{b} \notin \mathbb{F}_q$. Then $x^2 - b$ is the minimal polynomial of b and so $\mathbb{F}_q(\sqrt{b})$ is a quadratic extension. Hence $\mathbb{F}_q(\sqrt{b}) = \mathbb{F}_{q^2}$.
2. Let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ be given by $\varphi(a) = a^2$. If $q \equiv 0 \mod 3$ then φ is a field isomorphism and so $\mathbb{F}_q(\sqrt[3]{b}) = \mathbb{F}_q$ for all $b \in \mathbb{F}_q$. If $q \equiv 1 \mod 3$ then $\left|\mathbb{F}_q^*\right| \equiv 0 \mod 3$. Hence there exists an element $a \in \mathbb{F}_q$ of order three so $\varphi(a) = 1 = \varphi(1)$ and so φ is not injective. It follows that there exists $b \in \mathbb{F}_q$ such that $\sqrt[3]{b} \notin \mathbb{F}_q$. Then $F_q(\sqrt[3]{b})$ is a cubic extension and so it is equal to F_{q^3}. Lastly if $q \equiv 2 \mod 3$ then $\left|\mathbb{F}_q^*\right| \equiv 1 \mod 3$ and so there is no element of order three in $\mathbb{F}_q$. Then for $a, b \in \mathbb{F}_q$ such that $\varphi(a) = \varphi(b)$ we have

$$\begin{aligned} 1 &= \varphi(aa^{-1}) \\ &= \left(aa^{-1}\right)^3 \\ &= a^3\left(a^{-1}\right)^3 \\ &= \left(ba^{-1}\right)^3 \end{aligned}$$

and so $ba^{-1} = 1$ since there is not element of order 3 in $\mathbb{F}_q$. Therefore φ is injective hence surjective and so every element has a cube root. It follows that $\mathbb{F}_q(\sqrt[3]{b}) = \mathbb{F}_q, \forall b \in \mathbb{F}_q$.

Exercise 22.13
Let p be an odd prime.

1. Show that $\mathbb{F}_{p^2}$ contains a primitive eighth root of unity ζ and that $\alpha = \zeta + \zeta^{-1}$ satisfies $\alpha^2 = 2$.

2. Prove: $\alpha \in \mathbb{F}_p \iff p \equiv \pm 1 \mod 8$. Conclude that 2 is a square modulo p if and only if $p \equiv \pm 1 \mod 8$.

Proof.

1. Since $p^2 - 1 = (p-1)(p+1)$ is a product of two consecutive even numbers it follows that $8 \mid p^2 - 1$ and so there exists an element $\zeta \in \mathbb{F}_{p^2}^*$ of order 8. Let $\alpha = \zeta + \zeta^{-1}$. Then $\alpha^2 = \zeta^2 + 2 + \zeta^{-2}$. Noting that $\zeta^4 = -1$ we have

$$\begin{aligned}\left(\zeta^2 + \zeta^{-2}\right)^2 &= \zeta^4 + 2 + \zeta^{-4} \\ &= 2\zeta^4 + 2 \qquad\qquad (\text{Since } \zeta^{-4} = \zeta^4) \\ &= 0\end{aligned}$$

   and so $\alpha^2 = 2$.

2. Suppose $p \equiv \pm 1 \mod 8$. Then

$$\begin{aligned}\alpha^p &= \zeta^p + \zeta^{-p} \\ &= \zeta^{8k \pm 1} + \zeta^{-8k \mp 1} \\ &= \zeta^{\pm 1} + \zeta^{\mp 1} \\ &= \alpha\end{aligned}$$

   and so $\alpha \in \mathbb{F}_p$ as $\mathbb{F}_p = \{a \in \mathbb{F}_{p^2} \mid a^p = a\}$. This proves that $p \equiv \mod 8 \implies 2$ is a square modulo p.

   Conversely suppose that $p \not\equiv \pm 1 \mod 8$. Since p can't be congruent to 0,2,4 or 6 modulo 8 it follows that $p \equiv 3 \mod 8$ or $p \equiv 5 \mod 8$. Equivalently, $p \equiv \pm 3 \mod 8$. So we have

$$\begin{aligned}\alpha^p &= \zeta^p + \zeta^{-p} \\ &= \zeta^{8k \pm 3} + \zeta^{-8k \mp 3} \\ &= \zeta^{\pm 3} + \zeta^{\mp 3} \\ &= \zeta^3 + \zeta^{-3} \\ &= \zeta^4\left(\zeta^{-1} + \zeta^{-7}\right) \\ &= \zeta^4\left(\zeta^{-1} + \zeta^1\right) \\ &= -\alpha.x\end{aligned}$$

   So $\alpha \notin \mathbb{F}_p$. Since $\pm\alpha$ are the roots of 2 in $\mathbb{F}_{p^2}$, it follows that 2 is not a square in $\mathbb{F}_p$.

□

Exercise 22.15
Determine all the primes for which $\mathbb{F}_p[x]/(x^4+1)$ is a field.

Solution. If $p = 2$ then $x^4+1 = (x^2+1)^2 = (x+1)^4$ so p is odd. Then x^4+1 divides x^8-1 in $\mathbb{F}_p[x]$. Since $p^2-1 = (p+1)(p-1)$ is a product of two consecutive even numbers it follows that $8 \mid p^2-1$. Hence x^8-1 splits completely in $\mathbb{F}_{p^2}[x]$. So

$$x^8-1 = (x-1)(x-\beta)\cdots(x-\beta^7) = (x^4+1)(x^4-1)$$

for some $\beta \in \mathbb{F}_{p^2}$. If x^4+1 is irreducible in $\mathbb{F}_p[x]$, then for any root α of x^4+1, $\mathbb{F}_p(\alpha)$ is an extension of degree four. But x^4+1 splits completely in a quadratic extension and so it is reducible in $\mathbb{F}_p[x]$.

Alternative solution

If -1 is a square in $\mathbb{F}_p$ then $a^2 = -1$ for some $a \in \mathbb{F}_p$. So

$$x^4+1 = x^4-a^2 = (x^2+a)(x^2-a).$$

If 2 is a square in $\mathbb{F}_p$ then $b^2 = 2$ for some $b \in \mathbb{F}_p$ and so

$$x^4+1 = (x^2+1)^2-(bx)^2 = (x^2+1+bx)(x^2+1-bx).$$

Lastly, if neither -1 nor 2 are squares in $\mathbb{F}_p$, then p is odd (since $-1 = 1 = 1^2$ in $\mathbb{Z}/2\mathbb{Z}$). Then $\mathbb{F}_p^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ is cyclic subgroup of even order. Since -1 and 2 are odd powers of α, it follows that their product -2 is an even power of α and so it is a square. So let $c \in \mathbb{F}_p$ such that $c^2 = -2$. Then

$$x^4+1 = (x^2-1)-(cx)^2 = (x^2-1-cx)(x^2-1+cx).$$

Therefore x^4+1 is reducible modulo every prime.

Exercise 22.16
Prove: $f(x) = x^3+2$ is irreducible in $\mathbb{F}_{49}[x]$. Is f irreducible over $\mathbb{F}_{7^n}$ for all even n?

Proof. Let $\alpha \in \overline{\mathbb{F}_7}$ be a root of f. Then $\alpha^3 = -2$ and so $\alpha^{18} = 1$. Since $\alpha^9 = -1$ and $\alpha^6 = 4$ it follows that the order of α is 18. Hence $\alpha \in \mathbb{F}_{7^m} \iff 18 \mid 7^m-1$. Therefore $7^m \equiv 1 \mod 18$ and by the Chinese Remainder Theorem and the fact that 7^m is always odd it follows that $7^m \equiv 1 \mod 3$. Since the order of 7 is 3 in $\mathbb{Z}/3\mathbb{Z}$ ($7^3 = 7\cdot 7^2 = 7\cdot 49 = 7\cdot 4 = 28 = 1$) it follows that $3 \mid m$. Then $\alpha \in \mathbb{F}_{7^3}$. Since the degrees of the extensions $\mathbb{F}_{7^2}/\mathbb{F}_7$ and $\mathbb{F}_{7^3}/\mathbb{F}_7$ are coprime it follows that $[\mathbb{F}_{7^2}(\alpha) : \mathbb{F}_{7^2}] = 3$. Hence $\deg f^{\alpha}_{\mathbb{F}_{7^2}} = 3$ and $f \mid f^{\alpha}_{\mathbb{F}_{7^2}}$. Since f is a monic polynomial of degree 3 it follows that $f = f^{\alpha}_{\mathbb{F}_{7^2}}$ and so it is irreducible over $\mathbb{F}_{7^2}[x]$.

Lastly, it is not true that f is irreducible in $\mathbb{F}_{7^n}$ for all even n since $F_{7^3} \subset \mathbb{F}_{7^6}$ and we already showed that f has a root in $\mathbb{F}_{7^3}$. □

Exercise 22.17
Prove: $f(x) = x^4+2$ is irreducible in $\mathbb{F}_{125}[x]$. Is f irreducible over $\mathbb{F}_{5^n}$ for all n odd?

Proof. Let $\alpha \in \overline{\mathbb{F}_5}$ be a root of f. Then $\alpha^4 = -2$ and so $\alpha^16 = 1$. Since $\alpha^{\frac{16}{2}} = \alpha^8 = (-2)^2 = 4$ it follows that the order of α is 16. Then f has a root in $\mathbb{F}_{5^m} \iff 16 \mid 5^m - 1$. Thus $5^m \equiv 1 \mod 16$ and so $4 \mid m$ since 5 has order 4 in $\mathbb{Z}/16\mathbb{Z}$. Then $\alpha \in \mathbb{F}_{5^4}$ and so $\deg f^{\alpha}_{\mathbb{F}_5} = 4$ and $f^{\alpha}_{\mathbb{F}_5} \mid f$. But f is a monic polynomial of degree 4 and so $f = f^{\alpha}_{\mathbb{F}_5}$.

Let n be an odd number. Since $\mathbb{F}_5(\alpha) = \mathbb{F}_{5^4}$ is an extension of degree 4, and $\gcd(4, n) = 1$ it follows that $[\mathbb{F}_{5^n}(\alpha) : \mathbb{F}_{5^n}] = 4$ and so $\deg f^{\alpha}_{\mathbb{F}_{5^n}} = 4$ and $f^{\alpha}_{\mathbb{F}_{5^n}} \mid f$. Since f is a monic polynomial of degree 4, $f = f^{\alpha}_{\mathbb{F}_{5^n}}$ and so f is irreducible in $\mathbb{F}_{5^n}[x]$ for n odd. □

Exercise 22.19
Let $F = \mathbb{F}_{2^5}$.

1. Prove: for all $x \in F \setminus \mathbb{F}_2$, we have $F^* = \langle x \rangle$.
2. For how many polynomials $f \in \mathbb{F}_2[x]$ do we have $\mathbb{F}_2[x]/(f) \simeq F$?

Solution.

1. Let $x \in F \setminus \mathbb{F}_2$. Then the order of x divides $31 = 2^5 - 1$, i.e. the order of x is 1 or 31. Since $x \neq 1 \in \mathbb{F}_2$ it follows that $|x| = 31$ and so $\langle x \rangle = F^*$.
2. Since $\mathbb{F}_2[x]/(f) \simeq F$ if and only if f is an irreducible polynomial of degree 5, we need to find the number of degree five irreducible polynomials in $\mathbb{F}_2$. If x_d is the number of monic irreducible polynomials of degree d in $\mathbb{F}_2[x]$ than
$$32 = \sum_{d|5} d \cdot x_d = 2 + 5x_5.$$
Hence the number of irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$ is $x_5 = 6$.

Exercise 22.24
Show that there exists $\frac{p^2+p}{2}$ monic polynomial of degree 2 in $\mathbb{F}_p[x]$ that are reducible. Conclude, $x_2 = \frac{p^2-p}{2}$. Also determine x_3.

Solution. All the monic reducible polynomials of degree 2 have the form $(x - a)(x - b)$. If $a = b$ there are p choices. If $a \neq b$ then there are $\binom{p}{2} = \frac{p(p-1)}{2}$. Hence there are
$$\frac{p^2 + p}{2}$$
monic reducible polynomials of degree 2 in $\mathbb{F}_p[x]$. Since all monic polynomials of degree 2 have the form $x^2 + ax + b$, there are p^2 such polynomials. Hence $x_2 = p^2 - \frac{p^2+p}{2} = \frac{p^2-p}{2}$.

Similarly, the total number of degree 3 monic polynomials is p^3. There are 4 types of reducible monic polynomials of degree 3:

$$(x - a)^3, (x - a)^2(x - b), (x - a)(x - b)(x - c), \text{and } (x - a)(x^2 + bx + c).$$

There are $\binom{p}{1}$ of the first type $2\binom{p}{2}$ of the second (since twice a and once b is different to once a and twice b), $\binom{p}{3}$ of the third type and $p\frac{p^2-p}{2}$ of the fourth type ($\frac{p^2-p}{2}$ irreducible polynomials of degree 2 by the previous paragraph). Putting it all together we get

$$x_3 = p^3 - \binom{p}{1} - 2\binom{p}{2} - \binom{p}{3} - p\frac{p^2-p}{2} = \frac{p^3-p}{3}.$$

Exercise 22.30
Prove that $f(x) = x^p - x - a \in \mathbb{F}_p[x]$ is irreducible for all $a \in \mathbb{F}_p^*$. How does the polynomial $x^q - x - a \in \mathbb{F}_q[x]$ decompose into irreducible factors for an arbitrary finite field $\mathbb{F}_q$?

Proof. Since for any $k \in \mathbb{F}_p$, $k^p - k = 0$ and $a \neq 0$ by assumption, thus f has not roots in $\mathbb{F}_p$. So let $\alpha \in \overline{\mathbb{F}_p}$ be a root of f. Since $f' = -1$, f has p distinct roots. Observe that for any $k \in \mathbb{F}_p$ we have

$$\begin{aligned} f(\alpha + k) &= (\alpha + k)^p - (\alpha - k) - a \\ &= \alpha^p + k^p - \alpha - k - a \\ &= \alpha^p - \alpha - a && \text{(Since } k^p = k\text{)} \\ &= 0 \end{aligned}$$

and so all the zeros of f are of the form $\alpha + k$ for $k \in \mathbb{F}_p$. Let $f = g_1 \cdots g_n$ for $g_1, \ldots, g_n$ irreducible over $\mathbb{F}_p[x]$. Then each g_i must be the minimal polynomial of at least one of the roots of f. Since

$$\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + k)$$

for all $k \in \mathbb{F}_p$ it follows that the degree of all the g_i must the same. Hence $p = \deg f = n \deg g$. We know that $\deg g \neq 1$ since f has no roots in $\mathbb{F}_p$ and therefore $n = 1$ so f is irreducible.

Consider $f(x) = x^q - x - a \in \mathbb{F}_q[x]$ where $q = p^n$ and let $\alpha \in \overline{\mathbb{F}_p}$ be a root of f. Then $\alpha^q = \alpha + a$ and suppose $\alpha^{q^i} = \alpha + ia$. Then

$$\begin{aligned} \alpha^{q^{i+1}} &= \left(\alpha^{q^i}\right)^q \\ &= (\alpha + ia)^q && \text{(induction hypothesis)} \\ &= \alpha^q + (ia)^q && \text{(Frobenius)} \\ &= \alpha + (i+1)a && \text{(since } \alpha \text{ is a root of } f\text{)} \end{aligned}$$

which completes the induction. Since $\alpha^{q^p} = \alpha + pa = \alpha$ it follows that

$$f^{\alpha}_{\mathbb{F}_q}(x) = \prod_{i=0}^{p-1} \left(x - \alpha^{q^i}\right) = \prod_{i=0}^{p-1} (x - \alpha - ia) \in \overline{\mathbb{F}_p}[x]$$

is a degree p polynomial.

□

Exercise 22.31
Let $K \subset L$ be an extension of finite fields and $G = \mathrm{Aut}_K(L)$ the associated automorphism group. Prove: for $\alpha \in L$ with $L = K(\alpha)$ we have $f_K^\alpha = \prod_{\sigma \in G}(x - \sigma(\alpha))$. What is the corresponding statement for an arbitrary $\alpha \in L$?

Proof. Let K be a finite field, $L = K(\alpha)$ and $f(x) = \sum_{i=0}^n a_i x^i$ the minimal polynomial of α in $K[x]$. Let $\sigma \in G$ be a field automorphism, then

$$\begin{aligned} f(\sigma(\alpha)) &= \sum_{i=0}^n a_i \sigma(\alpha)^i \\ &= \sum_{i=0}^n \sigma(a_i \alpha^i) && \text{(since } \sigma(a) = a, \forall a \in K\text{)} \\ &= \sigma\left(\sum_{i=0}^n a_i \alpha^i\right) \\ &= \sigma(f(\alpha)) \\ &= 0, \end{aligned}$$

and so $\sigma(\alpha)$ is a root of f. □

Exercise (extra)
Let K be a field, $\overline{K}$ and algebraic closure and $f \in K[x]$ a non-constant polynomial. Then f has no repeated roots in $\overline{K}$ if and only if f is coprime to f'.

Proof. ($\Leftarrow$) Suppose f has a repeated roots in $\overline{K}$. Then

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

for $n \geq 2$. Taking the derivative we get

$$f'(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n g'(x) = (x - \alpha)^{n-1}\big(ng(x) + (x - \alpha)g'(x)\big)$$

so $(x - \alpha)^{n-1}$ divides both f and f' so they are not coprime.

($\Rightarrow$) Conversely suppose that f and f' are not coprime. Let $\gcd(f, f') = (x - \alpha)d(x)$ and let $\alpha \in \overline{K}$ be a root of d. Then $f(x) = (x - \alpha)h(x)$ and $f'(x) = (x - \alpha)h'(x) + h(x)$. Since $d(\alpha) = 0$, $f'(\alpha) = 0$ and so $h(\alpha) = 0$. Hence $h(x) = (x - \alpha)h_1(x)$ and $f(x) = (x - \alpha)^2 h_1(x)$. Hence α is a double root of f. □

Separable and Normal Extensions