1. Warm-up

Definition 1. An integral domain is a commutative ring with unit that has no zero-divisors, namely there are no nonzero elements \(a,b\) such that \(ab = 0\). A field is an integral domain where moreover any nonzero element has a multiplicative inverse. The characteristic of a domain is the smallest nonzero number \(n\) such that \(n1 = 0\), or 0 if there is none.

Exercise 1. The characteristic of an integral domain is either 0 or a prime number.

Exercise 2. Every field contains either \(\mathbb{Q}\) or \(\mathbb{Z}/p\mathbb{Z}\) for some prime \(p\).

Definition 2. If \(K\) and \(L\) are fields, and \(K \subset L\), we say that \(L\) is an extension of \(K\). We can think of \(L\) as a vector space over \(K\). The dimension of this space is called the degree of the extension, denoted \([L : K]\).

An element \(a \in L\) is called algebraic over \(K\), if there is a nonzero polynomial \(p(T) \in K[T]\) such that \(p(a) = 0\). It is called transcendental, if not. The extension is called algebraic, if every element is algebraic over \(K\), and transcendental otherwise.

If \(K \subset L \subset M\), then \([M : K] = [M : L][L : K]\).

Exercise 3. A finite extension is algebraic.

Exercise 4. (1) All ideals in \(K[T]\) are principal.

(2) The ideal \((f)\) is maximal if and only if \(f\) is irreducible

(3) For any \(a \in L\), there is a homomorphism \(K[T] \rightarrow L\) sending \(T\) to \(a\). Let \((p(T))\) be its kernel. Then \(p(T)\) is irreducible.

(4) Let \(p(T)\) be an irreducible polynomial. Then \(K[T]/(p(T))\) is a field extension of \(K\), where \(p(T)\) has a solution. What is the degree of the extension?

Definition 3. Let \(E \subset L\) be a set. Say that \(L\) is generated by \(E\), if \(K(E) = L\), where \(K(E)\) is the smallest subfield of \(L\) containing \(K\) and \(E\).

Exercise 5. Show that, if \(a,b\) are algebraic, then so are their sum, product and quotient.

2. Separability, Perfect fields

From now on we only deal with algebraic extensions.

Definition 4. An extension is separable, if the minimal polynomial of every element of the extension is separable, namely it does not have multiple roots. A field is called perfect, if every algebraic extension of it is separable.

The primitive element theorem says that a finite separable extension is generated by one element.
Exercise 6 (*). A field is perfect if either it has characteristic 0 or it has characteristic $p$ and the morphism $a \rightarrow a^p$ is an automorphism.

Exercise 7. For a field of characteristic $p$, the map $x \rightarrow x^p$ is a field monomorphism. If the field is finite, then it is an isomorphism, called the Frobenius map.

Exercise 8. Let $L$ be a finite field.
   1. Show that $L$ contains the field $F_p = \mathbb{Z}/p\mathbb{Z}$ for some prime $p$.
   2. Show that then $q = |L| = p^k$ for some $k$.
   3. Show that for each $x \in L$, $x \neq 0$, we have $x^{q-1} = 1$.

3. Splitting fields, Algebraic Closure

Definition 5. A field extension $K \subset L$ is called a splitting field for a polynomial $f(T) \in K[T]$, if the polynomial splits into linear factors in $L$, and there is no smaller field with this property. Splitting fields exist and are unique up to isomorphism.

Exercise 9. Find a splitting field for $T^3 - 2$ over $\mathbb{Q}$. Find its degree.

Exercise 10. With notation as in exercise 8, show that $L$ is a splitting field for the polynomial $T^q - T$. Thus there is up to isomorphism a unique field with $q$ elements, for each $q = p^k$.

Example 6. Examples of field automorphisms
   1. Complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$
   2. The map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2})$

Exercise 11. Show that $L = \bigcup_n \mathbb{Q}(n\sqrt{2})$ is a field, and algebraic over $\mathbb{Q}$. Find all the $\mathbb{Q}$-automorphisms of $L$.

Exercise 12. Determine the group of automorphisms of $\mathbb{Q}(\sqrt{2}, \zeta)$ over $\mathbb{Q}$, where $\zeta$ is a primitive 3rd root of unity.

Definition 7. The algebraic closure of a field $K$ is an extension of $K$ that contains a root of every polynomial over $K$. Algebraic closures exist and are unique up to isomorphism.

Example 8. The fundamental theorem of algebra tells us that $\mathbb{C}$ contains an algebraic closure of $\mathbb{Q}$.

4. Normal-Galois extensions

Definition 9. An extension $L$ of $K$ is normal, if, for every element $a \in L$, the minimal polynomial of $a$ splits in $L$. Splitting fields of polynomials are normal extensions.

Let $G(L, K)$ be the set of all automorphisms of $L$ that are the identity on $K$. If $H \subset G(L, K)$ is a subgroup, the fixed field of $H$ is $\text{Fix } H = \{a \in L | \sigma(a) = a \text{ for all } \sigma \in H\}$. The extension is called Galois, if $\text{Fix}(G(L, K)) = K$.

A finite extension is Galois if and only if it is normal and separable.

Theorem 10 (Fundamental Theorem of Galois Theory). Let $L/K$ be a finite Galois extension. Let $E$ be the set of intermediate field extensions of $L$ and $K$, and $R$ the set of subgroups of the group $G = G(L, K)$. Set $F : E \rightarrow R$, $F(M) = G(L, M)$ and $T : R \rightarrow E$, $T(H) = \text{Fix } H$. Then:
(1) $E$ and $R$ are inverses of each other and are inclusion reversing. Moreover, $[L : M] = |G(L, M)|$.
(2) $M \in E$ is normal, if and only if $F(M)$ is a normal subgroup of $G$. Then, $G(M, K) = G(L, K)/G(L, M)$.

Exercise 13. Set $L = Q(\sqrt[3]{2}, \zeta_i)$. Show that $L/Q$ is Galois. Compute $\text{Gal}(L, Q)$, find its subgroups, the corresponding intermediate field extensions, and determine which of them are normal.

Exercise 14. With notation as in exercise 8, $\text{Gal}(L/F_p)$ is cyclic of order $k$, generated by $F$.

Exercise 15. Let $N/K$ be a finite Galois extension with Galois group $G$. Show that $G$ is the direct product of two groups if and only if there are intermediate normal extensions $L_1$, $L_2$ such that $L_1 \cap L_2 = K$ and $L_1L_2 = N$.

5. Additional exercises

Exercise 16. A polynomial in $\mathbb{Z}[T]$ is called primitive, if the greatest common divisor of its coefficients is 1.

(1) The product of primitive polynomials in $\mathbb{Z}[T]$ is primitive.
(2) A primitive polynomial in $\mathbb{Z}[T]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[T]$.

Exercise 17. Let $F(T) = \prod_i (T - x_i)$ and $G(T) = \prod_j (T - y_j)$. Define the resultant $\text{Res}(F, G) = \prod_{i,j} (x_i - y_j)$.

(1) The resultant of two polynomials in $k[T]$ lies in $k$.
(2) $\text{Res}(F, G) = \prod_i G(x_i)$.
(3) If $F = GQ + R$, then $\text{Res}(F, G) = \pm \text{Res}(G, R)$.
(4) Define the discriminant of a polynomial $P$ as $D(P) = (-1)^{n(n-1)/2} \text{Res}(P, P')$. Then $P$ has multiple roots if and only if $D(P) = 0$.
(5) If $F(T) = \prod_i (T - x_i)$, then show that $D(F) = \prod_{i<j} (x_i - x_j)^2$.
(6) Identify the polynomials of degree $\leq n$ in $\mathbb{C}$ with $\mathbb{C}^{n+1}$. The set of polynomials with only simple roots is an open subset.
(7) The set of $n \times n$-matrices with distinct eigenvalues is open.

Exercise 18. The structure of $U(n) = (\mathbb{Z}/n\mathbb{Z})^\times$.

(1) The order of $U(n)$ is $\phi(n)$.
(2) If $n = rs$, with $r, s$ relatively prime, then $U(n) = U(r) \times U(s)$, and thus $\phi : \mathbb{N} \to \mathbb{N}$ is a multiplicative function.
(3) $\phi(p^n) = p^{n-1}(p - 1)$ for a prime $p$.
   Assume $n = p^k$, $p$ an odd prime.
(4) $U(p)$ is cyclic.
(5) Consider an element $a$ in $U(n)$ that maps to a generator of $U(p)$ under the natural map $U(n) \to U(p)$. Then $a$ has order $p^t(p - 1)$ for some $t \leq k$. Conclude that $a^p$ has order $p - 1$.
(6) For each $r$, $(1 + p)^{p^{r-1}} \equiv 1 + p^{r+1} \mod p^{r+2}$. Conclude that $1 + p$ has order $p^{k-1}$ in $U(n)$.
(7) Use the elements of orders $p - 1$ and $p^{k-1}$ to show that $U(n)$ is cyclic.
   Assume $n = 2^k$, $k \geq 2$. 

(8) Show that $5^{2r} \equiv 1 + 2^{r+2} \mod 2^{r+3}$. Conclude that 5 has order $2^{k-2}$ in $U(n)$.

(9) Show that no power of 5 is equal to -1 in $U(n)$.

(10) Conclude that $U(n) = \mathbb{Z}/p^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Exercise 19.** Let $k = \mathbb{Q}$. Set $\Phi_d(T) = \prod_{\zeta}(T - \zeta)$, the product over all primitive $d$-th roots of unity. For each $n$, let $\zeta_n$ denote an $n$-th root of unity.

1. $\Phi_d(T) \in k[T]$.
2. $T^n - 1 = \prod_{d|n} \Phi_d(T)$.
3. Use Möbius inversion to show $\Phi_n(T) = \prod_{d|n} (T^d - 1)^{\mu(n/d)}$. Conclude that $\Phi_n(T) \in \mathbb{Z}[T]$.
4. Let $E$ be the set of roots of the minimal polynomial of a primitive $n$-th root of unity $\zeta$. Then $E$ is closed under raising to powers relatively prime to $n$.
5. $\Phi_n(T)$ is irreducible over $k$.
6. $k[\zeta]/k$ is Galois of order $\phi(n)$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$, in particular, it is abelian.

Let $\zeta_n$ be a primitive $n$-th root of unity.

7. $\sqrt{2} \in k[\zeta_4]$.
8. Assume $p > 2$ prime, $D$ the discriminant of $S(T) = (T^p - 1)/(T - 1)$. Then $D$ is a square of an element $d \in k[\zeta_p]$.
9. $S'(x) = px^{p-1}/(x - 1)$ for all roots $x$ of $S$. Deduce $D = (-1)^{(p-1)/2}p^{-2} \sqrt{p}/d$ or $\sqrt{p}/id$ is rational.
10. $k[\sqrt{2}, \zeta_n] = k[\zeta_{4n}]$ for all odd $n$.

Conclude that every quadratic extension is contained in a cyclotomic one.

The following exercise deals with separability.

**Exercise 20.** For an algebraic extension $K \subset L$, let $\sigma : K \to \bar{K}$ be an embedding of $K$ into its algebraic closure. We call separable degree of the extension the number of distinct embeddings of $L$ into $\bar{K}$ extending $\sigma$, and denote it $[L : K]_s$. It is independent of the choice of $\sigma$.

1. The separable degree is multiplicative for a tower of extensions, namely for $E \subset F \subset K$, $[F : E][E : F] = [L : K]_s$.
2. If $L = K(a)$, let $p(T)$ be the minimal polynomial of $a$. Then there exists an integer $d$ and a separable polynomial $q(T)$ with $p(T) = q(T^d)$. The separable degree of the extension is equal to the degree of $q$. We have that $[L : K]_s \mid [L : K]$ and they are equal if and only if $a$ is separable, if and only if the extension is separable.
3. If the extension is finite, then again $[L : K]_s \mid [L : K]$, with equality if and only if $L$ is generated over $K$ by separable elements, if and only if the extension is separable. Moreover, $[L : K]/[L : K]_s$ is a power of $p$, the characteristic of $K$.
4. There is a maximal separable extension of $K$ in $L$. It consists of all elements of $L$ that are separable over $K$. It is called the separable closure of $K$ in $L$.
5. Let $M$ be the separable closure of $K$ in $L$. Then the extension on $L$ over $M$ is purely inseparable, namely for every element $a \in L$ the minimal polynomial of $a$ has the form $(T - a)^{p^s}$. 
