Core topics for the algebra qual

The algebra group

March 17, 2025

We provide a summary of the essential topics that students are expected to master for the algebra qualification exam. These are the topics for the academic year 2024-2025.

1 Group theory

1.1 Group actions

1. Bijection between group actions of G on X and group homomorphisms from G to the symmetric group S_X.
2. Consequence: A non-trivial action on a small set gives us a normal subgroup. For example, normal core of a subgroup, and the following result: if $[G : H]$ is the smallest prime factor of $|G|$, then H is a normal subgroup.
3. Various useful actions:
   (a) $G \curvearrowright G/H$ by left-translations.
   (b) For every normal subgroup N of G, $G \curvearrowright N$ by conjugation.
   (c) G acts on the set of subgroups of G by conjugation.
4. The orbit-stabilizer theorem: suppose $G \curvearrowright X$, then
$$G/G_x \to G \cdot x, \quad gG_x \mapsto g \cdot x$$
is a bijection.
5. $\mathrm{Cl}(g) = [G : C_G(g)]$ where $\mathrm{Cl}(g)$ is the conjugacy class of g.
6. Number of conjugates of a subgroup H of G is $[G : N_G(H)]$.
7. Orbits form a partition and the quotient space X/G.
8. Class equation.
9. (Not) Burnside's theorem: $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$.

1.2 Actions of finite p-groups and the Sylow theorems

1. Suppose a finite group P is of order p^k where p is prime and $P \curvearrowright X$ where X is a finite set. Then $|X| \equiv |X^P| \pmod{p}$.

2. Cauchy's theorem. If p is a prime factor of the order of a group G, then G has an element of order p.

3. The first Sylow theorem. If $p^n || G|$ and $|P| = p^i$, then there are subgroups $P_1, \ldots, P_n$ of G such that

   (a) $P_1 \subseteq \cdots \subseteq P_n$ and $P_i = P$.

   (b) $|P_j| = p^j$ for all $1 \leq j \leq n$.

4. The second Sylow theorem. $G \curvearrowright \mathrm{Syl}_p(G)$ by conjugation and this action is transitive.

5. The third Sylow theorem. $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$.

6. For every $P \in \mathrm{Syl}_p(G)$, $\mathrm{Syl}_p(N_G(P)) = \{P\}$ and deduce that
$$N_G(N_G(P)) = N_G(P).$$

7. Frattini's argument. Suppose $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$. Then
$$G = N_G(P)N.$$

8. Structure of groups of order pq if $p < q$ are primes and $p \nmid q - 1$.

9. Consequences of Sylow's theorems for groups of order $p(p-1)$, $p(p+1)$, p^2q, $pq\ell$, etc.

1.3 Short exact sequences and semi-direct product

1. Every SES is isomorphic to a standard SES.

2. A SES $1 \to G_1 \to G_2 \to G_3 \to 1$ splits if and only if there is an isomorphism $(\mathrm{id}_{G_1}, \phi, \mathrm{id}_{G_3})$ to the SES
$$1 \to G_1 \to G_1 \rtimes_\theta G_3 \to G_3 \to 1$$
for some $\theta : G_3 \to \mathrm{Aut}(G_1)$.

3. Structure of groups of order pq.

4. Suppose $\theta_1, \theta_2 \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ are in the same $\mathrm{Aut}(H)$-orbit. Then $H \ltimes_{\theta_1} N \simeq H \ltimes_{\theta_2} N$.

5. The Schur-Zassenhaus theorem. If $\gcd(|N|, |H|) = 1$, a SES of the form $1 \to N \to G \to H \to 1$ splits .

1.4 Symmetric and alternating groups

1. Cycle decomposition. Cycle type and conjugacy classes in a symmetric group.
2. Transpositions and parity of permutations.
3. $Z(S_n) = 1$ if $n \geq 3$.
4. 3-cycles generated the alternating group A_n if $n \geq 3$.
5. A_n is simple if $n \geq 5$.
6. $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ if $n \geq 7$.
7. Outer automorphism of S_6.
8. Sign of the permutation induced by the action of g on G by left multiplication and using it to show: if $|G| = 2m$ and m is odd, then G has a characteristic subgroup of order m.

1.5 Composition factors and solvable groups

1. The Jordan-Hölder theorem: for finite groups. For every finite group G, there are subgroups $\{G_i\}_i$ such that

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$$

   and G_i/G_{i-1} is a simple group for every $i = 1..k$. Up to reordering and isomorphisms, the quotients $\{G_i/G_{i-1}\}_{i=1}^k$ are unique and called the composition factors.
2. Derived subgroup series and solvable groups.
3. G/N is abelian if and only if $N \supseteq [G, G]$.
4. A finite group G is solvable if and only if all the composition factors are cyclic groups of prime order.
5. Important examples of solvable groups: dihedral groups and upper-triangular invertible n-by-n matrices.

1.6 Nilpotent groups

1. The lower and upper central series; denoted by $\gamma_i(G)$ and $Z_i(G)$, respectively.
2. $Z_c(G) = G$ if and only if $\gamma_{c+1}(G) = 1$.
3. Every finite p-group is nilpotent.

4. Suppose G is nilpotent and N is a non-trivial normal subgroup. Then

$$Z(G) \cap N \neq 1.$$

5. Important example for an infinite nilpotent group: group of unipotent upper-triangular matrices.

6. Suppose G is a finite group. Then the following are equivalent.

   (a) G is nilpotent.

   (b) All the Sylow subgroups of G are normal.

   (c) $G \simeq \prod_{i=1}^{n} P_i$ where P_i is a finite p_i-group.

   (d) All the maximal subgroups of G are normal.

7. Frattini subgroup and its properties. Let $\Phi(G)$ be the intersection of all the maximal subgroups of G. Suppose G is a finite group. Then

   (a) $\langle S \rangle = G$ if and only if $\langle \pi(S) \rangle = G/\Phi(G)$ where $\pi : G \to G/\Phi(G)$ is the natural quotient map.

   (b) $\Phi(G)$ is nilpotent.

   (c) G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.

   (d) If G is a finite p-group, then $\Phi(G) = [G, G]G^p$.

1.7 Free products, free groups, and ping-pong lemma

1. Free product of a family of groups and its universal property.

2. Free group and its universal property.

3. Presentation of a group. Important examples: dihedral and symmetric groups.

4. Ping-pong lemma and its applications:

   (a) $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ freely generate a free group.

   (b) $\left\langle \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq (\mathbb{Z}/2\mathbb{Z}) * \mathbb{Z}.$

   (c) Free groups are residually finite: if $w \in F_2 \setminus \{1\}$, then F_2 has a normal subgroup N of finite index such that $w \notin N$.

2 Ring theory

2.1 Ring of polynomials

1. Evaluation map. Leading term, leading coefficient, and degree.

2. Zero-divisors, units, integral domains, and fields.

3. Long division algorithm. Suppose A is a unital commutative ring, $f, g \in A[x]$, and the leading coefficient of g is a unit. Then there is a unique pair $(q, r) \in A[x]$ such that $f = gq + r$ and $\deg r < \deg g$.

4. Remainder and factor theorems. For every $f \in A[x]$ and $a \in A$, $f(x) = q(x)(x - a) + f(a)$; a is a zero of f if and only if $x - a | f$ in $A[x]$.

5. Generalized factor theorem. If D is an integral domain, $f \in D[x]$, and $a_1, \dots, a_n \in D$ are distinct zeros of f in D, then

$$f(x) = (x - a_1) \cdots (x - a_n) q(x)$$

   for some $q \in D[x]$.

2.2 Euclidean domains, PID, and UFD

1. Euclidean domain implies PID.

2. $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega]$, and $F[t]$ are Euclidean domains where ω is a primitive third root of unity and F is a field.

3. Primes and irreducible elements.

4. Prime and maximal ideals. An ideal $\mathfrak{p}$ of A is prime if and only if $A/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m}$ of A is maximal if and only if $A/\mathfrak{m}$ is a field. Hence

$$\mathrm{Max}(A) \subseteq \mathrm{Spec}(A).$$

5. Prime implies irreducible.

6. In an integral domain D and $a \neq 0$, a is prime if and only if $\langle a \rangle$ is a prime ideal; a is irreducible if and only if $\langle a \rangle$ is maximal among the principal ideals.

7. In a Noetherian integral domain, every non-zero non-unit element can be written as a product of irreducibles.

8. Suppose in an integral domain D, every non-zero non-unit element can be written as a product of irreducibles. Then D is a UFD if and only if irreducible and prime elements are the same.

9. PID implies UFD.

2.3 Prime and maximal ideals, and localization

For an ideal $\mathfrak{a}$, let $V(\mathfrak{a})$ be the set of prime divisors of $\mathfrak{a}$; that means

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

1. Zorn's lemma.

2. Suppose S is a multiplicatively closed subset, $\mathfrak{a} \trianglelefteq A$, and $S \cap \mathfrak{a} = \varnothing$. Then there exists $\mathfrak{p} \in V(\mathfrak{a})$ such that $\mathfrak{p} \cap S = \varnothing$.

3. For every proper ideal $\mathfrak{a}$, $V(\mathfrak{a}) \cap \mathrm{Max}(A) \neq \varnothing$.

4. Let $\mathrm{Nil}(A) := \{a \in A \mid \exists n \in \mathbb{Z}^+, a^n = 0\}$. Then $\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$.

5. $\mathrm{Nil}(A[x]) = \mathrm{Nil}(A)[x]$ and
$$A[x]^\times = \{\sum_{i=0}^n a_i x^i \mid a_0 \in A^\times, a_1, \ldots, a_n \in \mathrm{Nil}(A)\}.$$

6. Using $A[x]/\mathfrak{a}[x] \simeq (A/\mathfrak{a})[x]$ to deduce
$$\{\mathfrak{p}[x] \mid \mathfrak{p} \in \mathrm{Spec}(A)\} \subseteq \mathrm{Spec}(A[x]).$$

7. If D is a PID, then $\mathrm{Spec}(D) = \{0\} \cup \mathrm{Max}(D)$; as an application $A[x]$ is a PID if and only if A is a field.

8. Suppose S is multiplicatively closed. Then the following is a bijection:
$$\{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\} \to \mathrm{Spec}(S^{-1}A), \quad \mathfrak{p} \mapsto S^{-1}\mathfrak{p}.$$

9. For every $\mathfrak{p} \in \mathrm{Spec}(A)$, $S_\mathfrak{p} := A \setminus \mathfrak{p}$ is multiplicatively closed, and $S_\mathfrak{p}^{-1}A$ is denoted by $A_\mathfrak{p}$. We have $\mathrm{Max}(A_\mathfrak{p}) = \{S_\mathfrak{p}^{-1}\mathfrak{p}\}$; in particular, it is a local ring.

2.4 Noetherian rings and Hilbert's basis theorem

1. Noetherian rings. For every unital commutative ring A, the following properties are equivalent.
   (a) Every non-empty chain of ideals has a maximal element.
   (b) Every non-empty family of ideals has a maximal element.
   (c) Ascending chain condition (acc). If $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ is a chain of ideals of A, then there exists n_0 such that $\mathfrak{a}_{n_0} = \mathfrak{a}_{n_0+1} = \cdots$.
   (d) Every ideal of A is finitely generated.

2. Cohen's theorem. A is Noetherian if and only if every prime ideal of A is finitely generated.

3. If A is Noetherian, then every quotient of A is Noetherian.

4. Hilbert's basis theorem. If A is Noetherian, then $A[x]$ is Noetherian.

5. Every finitely generated ring is Noetherian.

2.5 Gauss's lemma

Suppose D is a UFD and F is a field of fractions of D.

1. Define p-valuations v_p and gcd. Basic properties of v_p and gcd.

2. The content $c(f)$ of a non-zero polynomial $f \in D[x]$. Primitive polynomials. For every non-zero polynomial $f \in D[x]$, we have

$$f = c(f) f_{\text{prim}},$$

   where f_{prim} is a primitive polynomial.

3. Gauss's lemma, version 1. Product of two primitive polynomials is primitive.

4. Gauss's lemma, version 2. $c(fg) = c(f)c(g)$ for $f, g \in D[x] \setminus \{0\}$.

5. Gauss's lemma, version 3. Suppose $f \in D[x]$, $f_1, \ldots, f_n \in F[x]$ such that $f = \prod_{i=1}^n f_i$. Then there exist $c_i \in F$ such that $c_i f_i \in D[x]$ and $f = \prod_{i=1}^n (c_i f_i)$.

6. Suppose f is a non-constant primitive polynomial in $D[x]$; then f is irreducible in $D[x]$ if and only if it is irreducible in $F[x]$.

7. For $a \in D$, we have a is irreducible (prime) in D if and only if a is irreducible (prime) in $D[x]$.

8. If D is a UFD, then $D[x]$ is a UFD.

3 Module and category theory

3.1 General theory of modules

1. There is a bijection between the possible A-module structures on an abelian group M and $\text{Hom}(A, \text{End}(M))$.

2. For a field F, F-modules are precisely F-vector spaces.

3. Suppose M is an A-module. For a multiplicatively closed set S, $S^{-1}M$ is a $S^{-1}A$-module. For $\mathfrak{p} \in \text{Spec}(A)$, $S_{\mathfrak{p}}^{-1}M$ is denoted by $M_{\mathfrak{p}}$.

4. Annahilator of an element and a module. An A-module M can be viewed as an $A/\text{Ann}(M)$-module, and this process does not change the POSet of submodules.

5. Quotient of modules and the isomorphism theorems.

6. Direct sum and direct product of modules, and their universal properties. Free A-modules.

7. Internal direct sum of submodules.
8. Noetherian modules. The following properties are equivalent.
   (a) Every non-empty chain of submodules of M has a maximal element.
   (b) Every non-empty family of submodules of M has a maximal element.
   (c) Ascending chain condition (acc). If $M_1 \subseteq M_2 \subseteq \cdots$ is a chain of submodules of M, then there exists n_0 such that $M_{n_0} = M_{n_0+1} = \cdots$.
   (d) Every submodule of M is finitely generated.
9. An epimorphism of a Noetherian module is an automorphism.
10. $\mathrm{rank}(M)$ is the maximum number of A-linearly independent elements of M and $d(M)$ is the minimum number of generators of M. Then, for a finitely generated A-module M, the following hold.
    (a) $\mathrm{rank}(M) \leq d(M)$.
    (b) $\mathrm{rank}(M) = d(M)$ if and only if M is a free A-module.

3.2 Finitely generated modules over a PID

Suppose D is a PID.

1. Submodules of a free module. Suppose M is a submodule of D^n. There are $a_1, \ldots, a_m \in D \setminus \{0\}$ and $v_1 \ldots, v_n \in D^n$ such that
   (a) $D^n = \bigoplus_{i=1}^n Dv_i$.
   (b) $a_1 | \cdots | a_m$ and $M = \bigoplus_{i=1}^m a_i D v_i$.
2. Fundamental theorem of f.g. modules over a PID. Suppose M is a f.g. D-module. Then there are non-negative integer r and $a_1, \ldots, a_m \in D \setminus \{0\}$ such that
   (a) $a_1 | \cdots | a_m$,
   (b) $\mathrm{M} \simeq D^r \oplus \bigoplus_{i=1}^m D/\langle a_i \rangle$,
   (c) $r = \mathrm{rank}(M)$,
   (d) $\mathrm{Tor}(M) \simeq \bigoplus_{i=1}^m D/\langle a_i \rangle$.

   Moreover, $\langle a_i \rangle$'s are unique.
3. Smith normal form. Suppose $x \in \mathrm{M}_{n,m}(D)$. Then there are $\gamma_1 \in \mathrm{GL}_n(D)$, $\gamma_2 \in \mathrm{GL}_m(D)$, and $d_1 | \cdots | d_r$ such that

   $$x = \gamma_1 a \gamma_2,$$

   where $a_{ii} = d_i$ and $a_{ij} = 0$ if $(i,j) \notin \{(1,1), \ldots, (r,r)\}$.
4. Application of Smith normal form in understanding the structure of the co-kernel of a D-module homomorphism from D^n to D^m.

3.3 Applications to linear algebra

Suppose F is a field and $a \in \mathrm{M}_n(F)$. Let $V_a := F^n$ be the $F[x]$-module such that $f(x) \cdot v = f(a)v$ for every column vector $v \in F^n$.

1. For $a, b \in \mathrm{M}_n(F)$, $a \sim b$ (that mean a is similar to b) if and only if $V_a \simeq V_b$.

2. For every monic polynomial $f \in F[x]$, $F[x]/\langle f \rangle \simeq V_{c(f)}$ where $c(f)$ is the companion matrix of f.

3. Rational canonical form. For every $a \in \mathrm{M}_n(F)$, there are unique monic polynomials $f_1, \ldots, f_m$ such that $f_1 | \cdots | f_m$ and

$$a \sim \mathrm{diag}(c(f_1), \ldots, c(f_m)).$$

   These polynomials are called the invariant factors of a.

4. Suppose $f_1 | \cdots | f_m$ are the invariant factors of a. Then f_m is the minimal polynomial of a and $f_1 \cdots f_m$ is the characteristic polynomial of a. In particular,

   (a) The Cayley-Hamilton Theorem. $f_a(a) = 0$ where $f_a(t) := \det(tI - a)$ is the characteristic polynomial of a.

   (b) The characteristic polynomial and the minimal polynomial of a have the same irreducible factors.

5. Jordan form. Suppose all the eigenvalues of f are in F. Then there are unique up to reordering pairs (n_i, λ_i) such that

$$a \sim \mathrm{diag}(J_{n_1}(\lambda_1), \ldots, J_{n_k}(\lambda_k)),$$

   where $J_m(\lambda) = \lambda I_m + c(x^m)$.

6. Two nilpotent matrices $x, x' \in \mathrm{M}_n(F)$ are similar if and only if

$$\dim \ker x^k = \dim \ker x'^k$$

   for every $k = 1..(n-1)$.

7. Suppose all the eigenvalues of a are in F. Then a is diagonalizable if and only if its minimal polynomial does not have a multiple zero.

8. The Smith form of $xI - a$ is of the form $\gamma_1 \,\mathrm{diag}(1, \ldots, 1, f_1, \ldots, f_r)\gamma_2$ such that $\gamma_1, \gamma_2 \in \mathrm{GL}_n(F[x])$ and $f_1 | \cdots | f_r$ are invariant factors of a.

3.4 A bit more general theory of modules

1. Nakayama's lemma, version 1. Suppose A is a local ring, $\mathrm{Max}(A) = \{\mathfrak{m}\}$, and M is a finitely generated A-module. If $\mathfrak{m}M = M$, then $M = 0$.

2. Nakayama's lemma, version 2. Suppose A is a local ring, $\mathrm{Max}(A) = \{\mathfrak{m}\}$, and M is a finitely generated ring. Then $d(M) = \dim_{A/\mathfrak{m}}(M/\mathfrak{m}M)$.

3. Every SES is isomorphic to a standard SES.

4. Suppose $0 \to M_1 \to M_2 \to M_3 \to 0$ is a SES. Then M_2 is Noetherian if and only if M_1 and M_3 are Noetherian.

5. Short five lemma. Suppose $(\theta_1, \theta_2, \theta_3)$ is a homomorphism of SESs; then the following holds.

   (a) θ_1, θ_3 are surjective if and only if θ_2 is surjective.

   (b) θ_1, θ_3 are injective if and only if θ_2 is injective.

   (c) θ_1, θ_3 are isomorphisms if and only if θ_2 is an isomorphism.

6. Splitting SES. Suppose $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ is a SES. Then the following statements are equivalent.

   (a) There exists a submodule N_2 of M_2 such that $N_2 \oplus f_1(M_1) = M_2$.

   (b) There exists $g_1 : M_2 \to M_1$ such that $g_1 \circ f_1 = \mathrm{id}_{M_1}$ (the left margin to the center and come back).

   (c) There exists $\theta : M_2 \to M_1 \oplus M_3$ such that $(\mathrm{id}_{M_1}, \theta, \mathrm{id}_{M_3})$ is an isomorphism of SESs between $0 \to M_1 \to M_2 \to M_3 \to 0$ and $0 \to M_1 \to M_1 \oplus M_3 \to M_3 \to 0$.

   (d) There exists $g_2 : M_3 \to M_2$ such that $f_2 \circ g_2 = \mathrm{id}_{M_3}$ (the right margin to the center and come back).

7. Suppose M is an A-module. Then the following are equivalent.

   (a) $M = 0$.

   (b) For all $\mathfrak{p} \in \mathrm{Spec}(A)$, $M_{\mathfrak{p}} = 0$.

   (c) For all $\mathfrak{m} \in \mathrm{Max}(A)$, $M_{\mathfrak{m}} = 0$.

8. Suppose $f : M \to N$ is an A-module homomorphism. Then the following are equivalent.

   (a) f is injective.

   (b) For all $\mathfrak{p} \in \mathrm{Spec}(A)$, $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective.

   (c) For all $\mathfrak{m} \in \mathrm{Max}(A)$, $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective.

9. Suppose $f : M \to N$ is an A-module homomorphism. Then the following are equivalent.

   (a) f is surjective.

   (b) For all $\mathfrak{p} \in \mathrm{Spec}(A)$, $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective.

   (c) For all $\mathfrak{m} \in \mathrm{Max}(A)$, $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective.

10. Suppose $\langle a_1, \ldots, a_m \rangle = A$ and M is an A-module. Then M is a finitely generated A-module if and only if $S_{a_i}^{-1}M$ is a finitely generated $S_{a_i}^{-1}A$-module for $i = 1..m$.

3.5 A bit of category theory

1. What a category is. Important examples: $\underline{\text{Set}}$ (sets), $\underline{\text{Gp}}$ (groups), $\underline{\text{Ab}}$ (abelian groups), A-$\underline{\text{mod}}$ (A-modules), $\underline{\text{Rng}}$ (unital commutative rings), etc.

2. What a functor is. Examples:

   (a) Forgetful functor. $F : \underline{\text{Gp}} \to \underline{\text{Set}}$, $F : \underline{\text{Ab}} \to \underline{\text{Gp}}$, etc.

   (b) Zeros of a family of polynomials. Suppose $\{f_i\}_{i\in I} \subseteq \mathbb{Z}[x_1, \dots, x_n]$. Then

   $$V_{\{f_i\}} : \underline{\text{Rng}} \to \underline{\text{Set}}, \quad V_{\{f_i\}}(A) := \{\mathbf{a} \in A^n \mid \forall i \in I, f_i(\mathbf{a}) = 0\}.$$

   (c) Group schemes. $\mathrm{GL}_n : \underline{\text{Rng}} \to \underline{\text{Gp}}$, $\mathrm{SL}_n : \underline{\text{Rng}} \to \underline{\text{Gp}}$.

   (d) Representable functor. Suppose $\mathrm{Hom}_{\mathcal{C}}(a, b)$ is a set for all objects a and b in $\mathcal{C}$. Then for all $a \in \mathrm{Ob}(\mathcal{C})$,

   $$h_a : \mathcal{C} \to \underline{\text{Set}}, h_a(b) := \mathrm{Hom}_{\mathcal{C}}(a, b),$$

   and

   $$h_a(b_1 \xrightarrow{f} b_2) : \mathrm{Hom}_{\mathcal{C}}(a, b_1) \to \mathrm{Hom}_{\mathcal{C}}(a, b_2)$$

   given by composition defines a functor.

3. What a natural transformation is. Examples:

   (a) Homomorphisms between group schemes. $\det : \underline{\mathrm{GL}_n} \to \underline{\mathrm{GL}_1}$ and inclusion map $\iota : \underline{\mathrm{SL}_n} \to \underline{\mathrm{GL}_n}$.

   (b) $\eta : \underline{\mathrm{GL}_1} \to V_{xy-1}$ such that $\eta_A(u) := (u, u^{-1})$.

4. Yoneda's lemma. Suppose $F : \mathcal{C} \to \underline{\text{Set}}$ is a functor and $\mathrm{Hom}_{\mathcal{C}}(a, b)$ is a set for all objects a and b in $\mathcal{C}$. Let $\mathrm{Nat}(h_a, F)$ be the class of all natural transformations from the representable functor h_a to F. Then there is a (natural) bijection between $\mathrm{Nat}(h_a, F)$ and $F(a)$.

3.6 Representable functors, projective modules, and tensor product

1. For a unital commutative ring A, the representable functor h_M can be upgraded to a functor from A-$\underline{\text{mod}}$ to A-$\underline{\text{mod}}$.

2. The contravariant representable functor, h^M can be enriched to a contravariant functor from A-$\underline{\text{mod}}$ to A-$\underline{\text{mod}}$.

3. h_M is right-exact; that means if $0 \to N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \to 0$ is a SES, then

   $$0 \to h_M(N_1) \xrightarrow{h_M(f_1)} h_M(N_2) \xrightarrow{h_M(f_2)} h_M(N_3)$$

   is exact.

4. h^M is right-exact; that means $0 \to N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \to 0$ is a SES, then

$$h^M(N_1) \xleftarrow{h^M(f_1)} h^M(N_2) \xleftarrow{h^M(f_2)} h^M(N_3) \leftarrow 0$$

is exact.

5. (Detecting exactness using observers-1) $N_1 \xrightarrow{f_1} \xrightarrow{f_2} N_3$ is exact if for all A-modules M, $h_M(N_1) \xrightarrow{h_M(f_1)} h_M(N_2) \xrightarrow{h_M(f_2)} h_M(N_3)$ is exact.

6. (Detecting exactness using observers-2) $N_1 \xrightarrow{f_1} \xrightarrow{f_2} N_3$ is exact if for all A-modules M, $h^M(N_1) \xleftarrow{h^M(f_1)} h^M(N_2) \xleftarrow{h^M(f_2)} h^M(N_3)$ is exact.

7. Projective modules. For an A-module P the following are equivalent.
   (a) h_P is an exact functor.
   (b) For every surjective A-module homomorphism f, $h_P(f)$ is surjective.
   (c) (Existence of a lift) Suppose $f : N_1 \to N_2$ is a surjective A-module homomorphism. Then for every $g \in \mathrm{Hom}_A(P, N_2)$, there exists $\widehat{g} \in \mathrm{Hom}_A(P, N_1)$ such that $g = f \circ \widehat{g}$.
   (d) Every SES of the form $0 \to M_1 \to M_2 \to P \to 0$ splits.
   (e) P is a direct summand of a free A-module.

8. Suppose D is an integral domain. Then a finitely generated ideal $\mathfrak{a}$ of D is a projective D-module if and only if there exists a finitely generated D-submodule $\mathfrak{b}$ of a field of fractions $Q(D)$ of D such that $\mathfrak{a}\mathfrak{b} = D$.

9. Functor of bilinear maps. Suppose M_1 and M_2 are two A-modules. Then there exists a natural isomorphism between the composite of representable functors h_{M_1} and h_{M_2}, and the functor b_{M_1,M_2} such that

$$b_{M_1,M_2}(N) := \{f : M_1 \times M_2 \to N \mid f \text{ is } A\text{-bilinear}\}.$$

10. Tensor product. $h_{M_1} \circ h_{M_2}$ is a representable functor; that means there is a natural isomorphism

$$h_{M_1} \circ h_{M_2} \simeq h_{M_1 \otimes_A M_2}.$$

11. Universal property of tensor product. $h_{M_1 \otimes_A M_2} \simeq b_{M_1,M_2}$ is equivalent to saying that for every A-bilinear $f : M_1 \times M_2 \to N$, there is a unique A-module homomorphism $\widehat{f} : M_1 \otimes_A M_2 \to N$ such that

$$\widehat{f}(x_1 \otimes x_2) = f(x_1, x_2).$$

12. Tensor-Hom adjunction. $h_{M_1} \circ h_{M_2} \simeq h_{M_1 \otimes_A M_2}$ is equivalent to saying that there is a natural isomorphism

$$\mathrm{Hom}_A(M_1, \mathrm{Hom}_A(M_2, N)) \simeq \mathrm{Hom}_A(M_1 \otimes_A M_2, N).$$

13. Tensor product of two projective modules is projective.

14. Distribution of tensor. There is a natural isomorphism

$$(\bigoplus_{i\in I} M_i) \otimes_A N \simeq \bigoplus_{i\in I} (M_i \otimes_A N).$$

15. A key isomorphism. There is a natural isomorphism

$$(A/\mathfrak{a}) \otimes_A M \simeq M/\mathfrak{a}M,$$

where $\mathfrak{a}$ is an ideal of A.

3.7 Tensor functor and flat modules

1. Existence of an A-module homomorphism $f \otimes g : M_1 \otimes_A N_1 \to M_2 \otimes N_2$ such that $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$, where $f \in \mathrm{Hom}_A(M_1, M_2)$ and $g \in \mathrm{Hom}_A(N_1, N_2)$.

2. For every A-module M, $T_M(N) := M \otimes_A N$ and $T_M(f) := \mathrm{id}_M \otimes f$ is a functor from A-mod to itself. When M is a (B, A)-bimodule (it is customary to write ${}_BM_A$), then T_M is also a functor from A-mod to B-mod.

3. T_M is a left adjoint of h_M; that means that for every A-modules N and K, there is a natural isomorphism

$$\mathrm{Hom}_A(T_M(N), K) \simeq \mathrm{Hom}_A(N, h_M(K)).$$

4. Suppose $\mathcal{F}, \mathcal{G}$ are two functors from A-mod to itself. Suppose $\mathcal{F}$ is the left adjoint of $\mathcal{G}$. Then $\mathcal{F}$ is right-exact and $\mathcal{G}$ is left-exact.

5. T_M is always right-exact.

6. Flat modules. The following statements are equivalent.

   (a) T_M is an exact functor.

   (b) If $f : N_1 \to N_2$ is injective, then $\mathrm{id}_M \otimes f : M \otimes_A N_1 \to M \otimes_A N_2$ is injective.

7. Tensor associativity. $T_{M_1} \circ T_{M_2} \simeq T_{M_1 \otimes_A M_2}$, and similar version for bimodules; this is equivalent to saying that there is a natural isomorphism

$$M_1 \otimes_A (M_2 \otimes_A N) \simeq (M_1 \otimes_A M_2) \otimes_A N.$$

8. Tensor product of two flat modules is flat.

9. $T_{\bigoplus_{i\in I} M_i} \simeq \bigoplus_{i\in I} T_{M_i}$; and so $\bigoplus_{i\in I} M_i$ is flat if and only if for all $i \in I$, M_i is flat.

10. Projective implies flat.

11. Locally flat if and only if flat; that means $M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for every $\mathfrak{p} \in \mathrm{Spec}(A)$ if and only if M is a flat A-module.

12. Suppose D is an integral domain. Then flat implies torsion free.

13. Suppose $0 \to M_1 \to M_2 \to M_3 \to 0$ is a SES and M_3 is flat. Then M_1 is flat if and only if M_2 is flat.

14. (Equation criterion) Suppose M is a flat A-module. Then if for some $\mathbf{m} \in \mathrm{M}_{n,1}(M)$ and $\mathbf{a} \in \mathrm{M}_{1,n}(A)$, we have

$$\mathbf{am} = 0,$$

then there are $B \in \mathrm{M}_{n,m}(A)$ and $\mathbf{y} \in \mathrm{M}_{m,1}(M)$ such that

$$\mathbf{a}B = 0 \quad \text{and} \quad B\mathbf{y} = \mathbf{m}.$$

15. The localization functor $S^{-1} : A\text{-}\underline{\mathrm{mod}} \to S^{-1}A\text{-}\underline{\mathrm{mod}}$ is exact.

16. (Commuting localization and representable functors (and tensor))

$$S^{-1} \circ h_M \simeq h_{S^{-1}M} \circ S^{-1} \quad \text{and} \quad S^{-1} \circ T_M \simeq T_{S^{-1}M} \circ S^{-1}.$$

17. Suppose M is a finitely presented A-module. Then M is flat if and only if it is locally free.

3.8 Tensor product and algebras

1. What an A-algebra is. Suppose B is a unital commutative ring. Then the following statements are equivalent.
   (a) There is a ring homomorphism $f : A \to B$ such that $f(1_A) = 1_B$.
   (b) B has an A-module structure which is compatible with its ring structure.

2. Suppose B is an A-algebra; then T_B is a functor from A-$\underline{\text{mod}}$ to B-$\underline{\text{mod}}$, and it is called a base change.

3. If B_1 and B_2 are two A-algebras, then the following product makes $B_1 \otimes_A B_2$ an A-algebra:

$$(b_1 \otimes b_2)(b'_1 \otimes b'_2) = (b_1 b'_1) \otimes (b_2 b'_2).$$

4. A key isomorphism. Suppose $\phi : A \to B$ is a ring homomorphism which makes B an A-algebra and $\mathfrak{a}$ is an ideal of $A[x]$. Then

$$B \otimes_A (A[x]/\mathfrak{a}) \simeq B[x]/B\phi(\mathfrak{a})$$

as B-algebras. In particular,

$$B \otimes_A (A[x]/\langle g_1, \ldots, g_n\rangle) \simeq B[x]/\langle \phi(g_1), \ldots, \phi(g_n)\rangle,$$

as B-algebras.

5. Chinese Remainder Theorem. Suppose $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise coprime ideals; that means $\mathfrak{a}_i + \mathfrak{a}_j = A$ if $i \neq j$. Then

$$A \Big/ \left(\bigcap_{i=1}^{n} \mathfrak{a}_i \right) \to \bigoplus_{i=1}^{n} A/\mathfrak{a}_i, \quad x + \left(\bigcap_{i=1}^{n} \mathfrak{a}_i \right) \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

is an A-algebra isomorphism.

6. If E/F is a field extension, $f \in F[x]$ factors into degree 1 polynomials over E, and it does not have multiple zeros, then

$$E \otimes_F (F[x]/\langle f\rangle) \simeq \underbrace{E \oplus \cdots \oplus E}_{\deg f\text{-times}},$$

as E-algebras.

4 Field theory

4.1 Basic properties of algebraic elements

1. Algebraic and transcendental elements in a field extension.

2. Suppose E/F is a field extension and $\alpha \in E$ is algebraic over F. Then the following statements hold.

   (a) Minimal polynomial. There is a unique monic polynomial $m_{\alpha,F} \in F[x]$ such that for $f \in F[x]$, $f(\alpha) = 0$ precisely when $m_{\alpha,F} | f$.

   (b) $m_{\alpha,F}$ is irreducible in $F[x]$. Conversely, if $p \in F[x]$ is irreducible, monic, and $p(\alpha) = 0$, then $p = m_{\alpha,F}$.

   (c) The F-algebra generated by α is a field and $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}\rangle$.

   (d) $(1, \alpha, \ldots, \alpha^{d-1})$ is an F-basis of $F[\alpha]$, where $d = \deg m_{\alpha,F}$; in particular
   $$[F[\alpha] : F] = \deg m_{\alpha,F}.$$

4.2 Finding zeros in a field extension

1. Existence – one root. Suppose $f \in F[x]$ is irreducible. Then there exists a pair (E, α) such that $E = F[\alpha]$ is a field and $f(\alpha) = 0$.

2. Isomorphism extension (uniqueness) – one root. Suppose $\theta : F \to F'$ is a field isomorphism, $f \in F[x]$ is irreducible, (E, α), and (E', α') are two pairs such that $E = F[\alpha]$, $E' = F'[\alpha']$, $f(\alpha) = 0$, and $f^{\theta}(\alpha') = 0$. Then there is an isomorphism $\widehat{\theta} : E \to E'$ which is an extension of θ and $\widehat{\theta}(\alpha) = \alpha'$.

$$\begin{array}{ccc} E & \overset{\widehat{\theta}}{\dashrightarrow} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\theta} & F' \end{array}$$

3. Existence – splitting field. Suppose $f \in F[x]$. Then there exist a field extension E/F, $\alpha_1, \ldots, \alpha_n \in E$ such that

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

and

$$E = F[\alpha_1, \ldots, \alpha_n].$$

4. Isomorphism extension (generalized uniqueness) – splitting field. Suppose $\theta : F \to F'$ is a field isomorphism, $f \in F[x]$, E is a splitting field of f over F, and E' is a splitting field of f^{θ} over F'. Then there is an isomorphism $\widehat{\theta} : E \to E'$ which is an extension of θ.

$$\begin{array}{ccc} E & \overset{\widehat{\theta}}{\dashrightarrow} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\theta} & F' \end{array}$$

Such an isomorphism $\widehat{\theta}$ is called a θ-isomorphism, and the set of all θ-isomorphisms is denoted by $\mathrm{Isom}_{\theta}(E, E')$. So $\mathrm{Isom}_{\theta}(E, E') \neq \varnothing$.

4.3 Basics of finite fields

1. If F is a finite field, then $\mathrm{char}(F) = p > 0$ and F is a vector space over $\mathbb{Z}/p\mathbb{Z}$.
2. Every finite field is of order p^n for some prime p and positive number n.
3. If F is a finite field, then $F^{\times}$ is cyclic.
4. For a prime power $q = p^n$, there is a unique up to an isomorphism field $\mathbb{F}_q$ of order q which is a splitting field of $x^q - x$ over $\mathbb{F}_p$.
5. $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

4.4 Separable polynomials

Separable polynomials. We say a polynomial $f \in F[x]$ is separable if f does not have multiple zeros in its splitting field over F.

1. f is separable if and only if $\gcd(f, f') = 1$.
2. If $f \in F[x]$ is irreducible and $f' \neq 0$, then f is separable. In particular, in the characteristic zero case, all irreducible polynomials are separable.
3. If $f \in F[x]$ and $\mathrm{char}(F) = p > 0$, then $f(x) = f_{\mathrm{sep}}(x^{p^k})$ for some non-negative integer k and separable polynomial $f_{\mathrm{sep}} \in F[x]$.

4.5 Finite Galois extensions

1. Tower formula. Suppose K is an intermediate subfield of E/F. Then
$$[E : F] = [E : K][K : F].$$
In particular, E/F is a finite extension if and only if both E/K and K/F are finite extensions.
2. A key theorem. Suppose $\theta : F \to F'$ is a field isomorphism, $f \in F[x]$, E is a splitting field of f over F, and E' is a splitting field of f^θ over F'. Then
$$|\mathrm{Isom}_\theta(E, E')| \leq [E : F],$$
and equality holds if all the irreducible factors of f are separable.
3. Suppose E/F and E/F' are field extensions and $\theta : F \to F'$ is an isomorphism. Then
$$|\mathrm{Isom}_\theta(E, E)| \leq [E : F].$$
In particular, $|\mathrm{Aut}_F(E)| \leq [E : F]$ for every finite field extensionE/F.
4. Normal extension. An algebraic extension E/F is called a normal extension if for every $\alpha \in E$, $m_{\alpha,F}$ factors into degree 1 polynomials in $E[x]$.
5. Separable extension. An algebraic extension E/F is called a separable extension if for every $\alpha \in E$, $m_{\alpha,F}$ is a separable polynomial.
6. Galois extension. An algebraic extension E/F is called a Galois extension if it is both normal and separable. For Galois extensions, we write $\mathrm{Gal}(E/F)$ instead of $\mathrm{Aut}_F(E)$.
7. A key theorem. Suppose E/F is a finite extension. Then the following statements are equivalent.
   (a) There exists a polynomial $f \in F[x]$ with separable irreducible factors such that E is a splitting field of f over F.
   (b) $|\mathrm{Aut}_F(E)| = [E : F]$.

(c) E/F is a Galois extension.

8. For every field extension E/F and $f \in F[x]$, $\mathrm{Aut}_F(E)$ acts on the set $Z_f(E)$ of zeros of f in E. If E/F is a finite Galois extension and $f \in F[x]$ is irreducible, then the action of $\mathrm{Gal}(E/F)$ on $Z_f(E)$ is transitive and the stabilizer of $\alpha \in Z_f(E)$ is $\mathrm{Gal}(E/F[\alpha])$.

9. If E is a splitting field of f over F, then $\mathrm{Aut}_F(E)$ can be embedded in the symmetric group of $Z_f(E)$.

10. Fundamental theorem of Galois theory – finite degree case. Suppose E/F is a finite Galois extension. Let $\mathrm{Int}(E/F)$ be the set of intermediate subfields and $\mathrm{Sub}(\mathrm{Gal}(E/F))$ be the set of all subgroups of $\mathrm{Gal}(E/F)$. Let

$$\Phi : \mathrm{Int}(E/F) \to \mathrm{Sub}(\mathrm{Gal}(E/F)), \quad \Phi(K) := \mathrm{Gal}(E/K),$$

and

$$\Psi : \mathrm{Sub}(\mathrm{Gal}(E/F)) \to \mathrm{Int}(E/F), \quad \Psi(H) := \mathrm{Fix}(H).$$

Then the following statements hold.

(a) Φ and Ψ are well-defined, and they are inverse of each other; that means

i. $E/\mathrm{Fix}(H)$ is Galois and $\mathrm{Gal}(E/\mathrm{Fix}(H)) = H$,

ii. G/K is Galois and $\mathrm{Fix}(\mathrm{Gal}(E/K)) = K$.

(b) Φ and Ψ are order-reversing.

(c) Φ and Ψ induce bijections between intermediate normal extensions and normal subgroups; that means

i. $E/\mathrm{Fix}(\mathrm{N})$ is a normal extension if and only if $N \trianglelefteq \mathrm{Gal}(E/F)$.

ii. $\mathrm{Gal}(E/K) \trianglelefteq \mathrm{Gal}(E/F)$ if and only if K/F is a normal extension.

iii. If K/F is a normal extension, then the following is a SES

$$1 \to \mathrm{Gal}(E/K) \to \mathrm{Gal}(E/F) \xrightarrow{r_{E,K}} \mathrm{Gal}(K/F) \to 1,$$

where $r_{E,K}$ is induced by restriction.

11. Normal extension criterion – weak version. Suppose E/F is a finite Galois extension and K is an intermediate subfield. Then the following statements are equivalent.

(a) K/F is normal.

(b) For every $\theta \in \mathrm{Gal}(E/F)$, $\theta(K) = K$.

(c) K is a splitting field of a polynomial $f \in F[x]$ over F.

4.6 Important examples of Galois extensions

1. Finite fields.
   (a) $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension.
   (b) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$, where $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \sigma_p(a) := a^p$ is the Frobenius endomorphism. In particular, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.
   (c) The following maps are bijections:

$$\mathrm{Int}(\mathbb{F}_{p^n}/\mathbb{F}_p) \longleftrightarrow \mathrm{Sub}(\langle \sigma_p \rangle) \longleftrightarrow D(n)$$

$$\mathbb{F}_{p^m} = \mathrm{Fix}(\sigma_p^m) \longleftrightarrow \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \sigma_p^m \rangle \longleftrightarrow |\langle \sigma_p^m \rangle| = n/m$$

   where $D(n)$ is the set of positive divisors of n.

2. Cyclic Kummer extensions. Suppose F is a field and $\zeta \in F$ has multiplicative order n. Suppose $a \in F^\times$. Let E be a splitting field of $x^n - a$ over F. Suppose $\sqrt[n]{a} \in E$ is a zero of $x^n - a$. Then the following statements hold.
   (a) $E = F[\sqrt[n]{a}]$ and E/F is Galois.
   (b) $\mathrm{Gal}(F[\sqrt[n]{a}]/F) \to \langle \zeta \rangle, \quad \theta \mapsto \frac{\theta(\sqrt[n]{a})}{\sqrt[n]{a}}$ is a well-defined injective group homomorphism. In particular, $\mathrm{Gal}(F[\sqrt[n]{a}]/F)$ is cyclic, and its order is a divisor of n.
   (c) $\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^\times)^n \rangle$.

3. General cyclotomic extensions. Suppose $n \geq 2$ is an integer and F is a field such that the characteristic of F is either 0 or a prime number which does not divide n. Let E be a splitting field of $x^n - 1$ over F.
   (a) The set of solutions of $x^n - 1 = 0$ in E is a cyclic group of order n; say $\zeta \in E^\times$ is of multiplicative order n. Then $E = F[\zeta]$.
   (b) $F[\zeta]/F$ is a Galois extension and for every $\theta \in \mathrm{Gal}(F[\zeta]/F)$, $\theta(\zeta)$ is a zero of $x^n - 1$ and so it is in $\langle \zeta \rangle$.
   (c) Restricting elements of the Galois group to the cyclic group $\langle \zeta \rangle$ gives us an injective group homomorphism $\mathrm{Gal}(F[\zeta]/F) \to \mathrm{Aut}(\langle \zeta \rangle)$. This implies that $\mathrm{Gal}(F[\zeta]/F)$ can be embedded into $(\mathbb{Z}/n\mathbb{Z})^\times$; in particular, $\mathrm{Gal}(F[\zeta]/F)$ is abelian.

4. Cyclotomic extensions. Let $\zeta_n := e^{2\pi i/n}$. Then $\mathbb{Q}[\zeta_n]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$. Let $\Phi_n(x) := \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^i)$; it is called the n-th cyclotomic polynomial.
   (a) $\prod_{d|n} \Phi_d(x) = x^n - 1$.
   (b) $\Phi_n(x) \in \mathbb{Z}[x]$.
   (c) $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$, and so $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$.

(d) $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times|$, and so $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

5. Using permutations. Suppose $f \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p, where p is a prime more than 3. Suppose f has exactly two non-real roots. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. Then

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq S_p.$$

4.7 Algebraic closure of a field

1. Suppose E/F is a field extension. Then

$$\{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E. It is called the algebraic closure of F in E.

2. Algebraically closed field. For a field F the following properties are equivalent.

   (a) Every non-constant polynomial in $F[x]$ has a zero in F.

   (b) Every non-constant polynomial in $F[x]$ factors as a product of degree 1 polynomials.

   (c) Every irreducible polynomial in $F[x]$ is of degree 1.

   (d) If E/F is an algebraic extension, then $E = F$.

3. Suppose E/F is a field extension and E is algebraically closed. Then the algebraic closure of F in E is an algebraically closed field.

4. Algebraic closure. For every field F, there exists an algebraically closed field $\overline{F}$ such that $\overline{F}/F$ is an algebraic extension.

5. Isomorphism extension. Suppose $\theta : F \to F'$ is a field isomorphism. Suppose $\overline{F}$ is an algebraic closure of F, and $\overline{F}'$ is an algebraic closure of F'. Then there exists an isomorphism $\widehat{\theta} : \overline{F} \to \overline{F}'$ which is an extension of θ.

$$\begin{array}{ccc} \overline{F} & \overset{\widehat{\theta}}{\dashrightarrow} & \overline{F}' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\ \theta\ } & F' \end{array}$$

4.8 Simple extensions

A field extension E/F is called a simple extension if there exists $\alpha \in E$ such that $E = F[\alpha]$.

1. Suppose E/F is a finite field extension. Then E/F is a simple extension if and only if there are only finitely many intermediate subfields; that means $|\mathrm{Int}(E/F)| < \infty$.

2. Galois closure and primitive element theorem. If E/F is a finite separable extension, then there exists a finite Galois extension K/F such that $E \subseteq K$. This implies that

$$|\text{Int}(E/F)| \leq |\text{Int}(K/F)| = |\text{Sub}(\text{Gal}(K/F))| < \infty.$$

Hence every finite separable extension is a simple extension.

4.9 Further results on separable extensions

1. Perfect fields. For a field F the following statements are equivalent.
   (a) Every algebraic extension E/F is separable.
   (b) Either the characteristic of F is zero or $\text{char}(F) = p > 0$ and $F^p = F$.

2. Purely inseparable extensions. Suppose E/F is a finite extension and $\text{char}(F) = p > 0$. Then the following statements are equivalent.
   (a) For every $\alpha \in E$, $m_{\alpha,F}(x) = x^{p^n} - a$ for some $n \in \mathbb{Z}^+$ and $a \in F$.
   (b) $E^\times/F^\times$ is a p-group.

3. If E/F is a finite purely inseparable extension and $\text{char}(F) = p > 0$, then $[E : F] = p^n$ for some $n \in \mathbb{Z}^+$.

4. Separable closure. Suppose E/F is a finite extension. Then

$$E_{\text{sep}} := \{\alpha \in E \mid m_{\alpha,F} \text{ is separable}\}$$

   is a field and E/E_{sep} is purely inseparable.

5. Tower of separable extensions. Suppose E/F is an algebraic extension and K is an intermediate field. Then E/F is separable if and only if E/K and K/F are separable.

4.10 Solvability by radicals

1. Dirichlet's independence of characters. Suppose E is a field and G is a group. Suppose $\chi_1, \ldots, \chi_n : G \to E^\times$ are non-trivial group homomorphisms. Then χ_i's are E-linearly independent.

2. Hilbert's theorem 90. Suppose $\text{Gal}(E/F) = \langle\sigma\rangle$. Then $N_{E/F}(a) = 1$ if and only if there exists $b \in E$ such that $a = \sigma(b)/b$.

3. Suppose $\text{char}(F) = 0$ and $f \in F[x]$. Let E be a splitting field of f over F. Then f is solvable by radicals if and only if $\text{Gal}(E/F)$ is a solvable group.