UIUC Algebra Comprehensive Exam Cheatsheet

Jiantong Liu

Aug 31, 2023

Introduction

I created this document in summer 2023 as an effort to prepare for the algebra comprehensive exam in August 2023, which I passed with 90/100. The document includes the important results I gathered based on the syllabus revised after August 2012. Note that the list may not be representative or comprehensive and should not be regarded as the exam's entire knowledge base. I have also included past comprehensive exam problems between May 2018 and May 2022, with problems attached at the end of their corresponding sections, to get a feeling of how often each topic occurs on the exam.

1 Group Theory

1.1 Isomorphism Theorems

Theorem 1.1.1 (Lagrange)**.** Let G be a finite group and H be a subgroup of G. Then the index $[G : H] = \frac{|G|}{|H|}$.

Definition 1.1.2. A subgroup H of G is normal $gH = Hg$ for all $g \in G$.

Proposition 1.1.3. Suppose H is a subgroup of G, then H is a normal subgroup of G if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

Proposition 1.1.4. If H is a normal subgroup of G, then G/H is a group with an induced group operation.

Proposition 1.1.5 (Universal Property)**.** Let $f : G \to H$ be a group homomorphism, and let $N \lhd G$ be a normal subgroup, then f factors through G/N if and only if $N \subseteq \ker(f)$.

Theorem 1.1.6 (First Isomorphism Theorem)**.** Let $f : G \to H$ be a group homomorphism, then $\ker(f) \lhd G$, and $G/\ker(f) \cong \mathrm{im}(f)$ is a group isomorphism.

Theorem 1.1.7 (Second Isomorphism Theorem)**.** Let G be a group, let $K \subseteq G$ be a subgroup, and $N \lhd G$ be a normal subgroup, then:

- KN is a subgroup of G;
- $N \lhd KN$ is a normal subgroup;
- $K \cap N \lhd K$ is a normal subgroup;
- $KN/N \cong K/(K \cap N)$ is a group isomorphism.

Theorem 1.1.8 (Third Isomorphism Theorem)**.** Let K and H be normal subgroups of a group G, and let $K \subseteq H$, then:

- $H/K \lhd G/K$ is a normal subgroup;

- $(G/K)/(H/K) \cong G/H$ is a group isomorphism.

Theorem 1.1.9 (Correspondence Theorem with preimage)**.** Let $f : G \to H$ be a surjective group homomorphism, and let $H' \subseteq H$ be a subgroup.

- Note that $f^{-1}(H') \subseteq G$ is a subgroup, and the assignments $H' \mapsto f^{-1}(H')$ gives a bijection between the set of subgroups of H and the set of subgroups of G containing $\ker(f)$.
- $H' \subseteq H$ is normal if and only if $f^{-1}(H') \subseteq G$ is normal. Moreover, $G/f^{-1}(H') \cong H/H'$ is an isomorphism of groups.

Theorem 1.1.10 (Correspondence Theorem with normal subgroups)**.** Let $N \lhd G$ be a normal subgroup, then the assignment $G \mapsto G/N$ of the canonical map gives

- a bijection between the set of all subgroups of G containing N, and the set of subgroups of G/N, and
- a bijection between the set of all normal subgroups of G containing N, and the set of all normal subgroups of G/N.

1.2 Group Actions

Definition 1.2.1 (Group Action)**.** Let G be a group and X be a set, then a (left) group action of G on X is a function

$$\begin{aligned} \varphi : G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

such that

- $e \cdot x = x$ for all $x \in X$, and
- for any $g, h \in G$ and $x \in X$, $g \cdot (h \cdot x) = (gh) \cdot x$.

Definition 1.2.2 (Orbit, Transitive)**.** Suppose G acts on X. Define a relation on X such that $x \sim x'$ if and only if $x' = gx$ for some $g \in G$. This is an equivalent relation. In particular, X is a disjoint union of equivalence classes, where we call each class an orbit. We would take a representative $x \in X$ from each orbit, and denote the class by $G \cdot x = \{g \cdot x \mid g \in G\}$.

We say a group action is transitive if there is only one orbit.

Definition 1.2.3 (Stabilizer)**.** Suppose G acts on X, and pick $x \in X$. The stabilizer of x of this action is $\mathrm{Stab}(x) = G_x = \{g \in G : g \cdot x = x\}$, which is a subgroup of G.

Example 1.2.4 (Left translation/multiplication)**.** Suppose $X = G$, then the left multiplication map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

defines a (faithful and transitive) group action.

Remark 1.2.5. Let $\Sigma(X)$ be the set of bijective set maps on a set X, then by fixing some $g \in G$, the action above induces a bijective set map $f_g : G \to G$ defined by $f_g(x) = gx$. Therefore, this induces an injective group homomorphism

$$\begin{aligned} f : G &\to \Sigma(G) \\ g &\mapsto f_g \end{aligned}$$

In particular, if G is a finite group of order n, then this identifies G to be a subgroup of S_n via $G \hookrightarrow S_n$.

Definition 1.2.6. The kernel of an action $G \times X \to X$ is the kernel of the induced group homomorphism $G \to \Sigma(X)$, thus the kernel is just the intersection $\bigcap_{x \in X} \mathrm{Stab}(x)$.

Example 1.2.7 (Coset action)**.** Let H be a subgroup of G, then let $X = G/H$ be the set of left cosets over H. There is an action

$$\begin{aligned} G \times X &\to X \\ (g, aH) &\mapsto (ga)H \end{aligned}$$

The orbit of $aH \in G/H$ is $X = G/H$; the stabilizer of $aH \in G/H$ is aHa^{-1}.

Example 1.2.8 (Conjugation action)**.** Suppose $X = G$, then the conjugation map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gxg^{-1} \end{aligned}$$

defines a group action. The orbit of $g \in G$ is the conjugacy class of $g \in G$; the stabilizer of $g \in G$ is the set $\{a \in G : aga^{-1} = g\}$, also known as the centralizer $C_G(g)$ of $g \in G$.

Remark 1.2.9. The conjugation action induces a function $G \to \Sigma(X)$ by $x \mapsto f_x$ just as above, where $f_x(g) = xgx^{-1}$. This is an automorphism. Moreover, an automorphism in the form of conjugation is called an inner automorphism. In particular, the function when restricting the codomain to $\mathrm{Aut}(G)$, defines a function $f : G \to \mathrm{Aut}(G)$, where the image is $\mathrm{Inn}(G)$.

Remark 1.2.10. The kernel of the induced homomorphism of the conjugation action is just the set $\{g \in G : gh = hg \, \forall h \in G\}$. This is known as the center $Z(G)$ of a group G.

Proposition 1.2.11. $Z(G) \lhd G$, and in particular $G/Z(G) \cong \mathrm{Inn}(G)$.

Example 1.2.12 (Conjugation action on subgroups)**.** Let X be the set of subgroups of G, then the function

$$\begin{aligned} G \times X &\to X \\ (g, H) &\mapsto gHg^{-1} \end{aligned}$$

is a group action. The orbit of $H \subseteq G$ is the set of subgroups gHg^{-1}; the stabilizer of $H \subseteq G$ is the set $\{g \in G : gHg^{-1} = H\}$, also known as the normalizer $N_G(H)$ of $H \subseteq G$.

Remark 1.2.13. The normalizer $N_G(H)$ is the largest subgroup of G with H as a normal subgroup. In particular, $H \lhd N_G(H)$.

Theorem 1.2.14 (Orbit-Stabilizer Theorem)**.** Let G act on X, and fix $x \in X$. The the cardinality of the orbit is $|G \cdot x| = [G : \mathrm{Stab}(x)]$.

Corollary 1.2.15. If G is finite, then the number of subgroups conjugate to $H \subseteq G$ is $\frac{|G|}{|N_G(H)|}$.

Exercise 1.2.16 (May 2022, Problem 1)**.** Let H be a subgroup of a group G. Then G acts on the set G/H by left multiplication. This action naturally defines a homomorphism $\alpha : G \to S(G/H)$, where $S(X)$ is the group of permutations on a set X. Prove that the kernel of α is contained in H.

Theorem 1.2.17 (May 2022, Problem 1; May 2019, Problem 1)**.** Let G be a finite group and p be the smallest prime divisor of $|G|$, then every subgroup H of G with index p is normal.

1.3 Class Equation

Definition 1.3.1 (Fixed point)**.** Let G be a group with an action on a set X. The set of fixed points of G on X is the subset $X^G = \{x \in X : g \cdot x = x \; \forall g \in G\}$ of X.

One can define the elements of X fixed by a particular element $g \in G$ similarly, and denote it by X^g.

Corollary 1.3.2 (Class equation of a group action)**.** Suppose G acts on X. Then

$$|X| = |X^G| + \sum_{i \in I} \frac{|G|}{G_i},$$

where G_i is the stabilizer of an orbit of size at least 2 and with representative s_i.

Corollary 1.3.3 (Class Equation)**.** Suppose G is a finite group, and let $C_1, \ldots, C_r$ be the conjugacy classes in $G \setminus Z(G)$. Pick representatives $g_i \in C_i$ for all i, then

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{C_G(g_i)}.$$

Remark 1.3.4. The center of a group is the set of fixed points on the group action of self-conjugation on G.

Lemma 1.3.5 (Burnside)**.** Suppose G is a finite group that acts on a set X. Let $X^g = \{x \in X \mid g \cdot x = x\}$, then the number of orbits $|X/G|$ is the average number of fixed points on elements, i.e.,

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Exercise 1.3.6 (August 2021, Problem 1)**.** Let G be a non-trivial finite group acting on a finite set X. We assume that for all $G \setminus \{e\}$ there exists a unique $x \in X$ such that $g \cdot x = x$.

(a) Let $Y = \{x \in X \mid G_x \neq \{e\}\}$ where G_x denotes the stabilizer of x. Show that Y is stable under the action of G.

(b) Let $y_1, y_2, \ldots, y_n$ be a set of orbit representatives of Y/G (with $|Y/G| = n$), and let $m_i = |G_{y_i}|$. Show that:

$$1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right)$$

(c) Show that X has (at least) a fixed point under the action of G.

Exercise 1.3.7 (August 2020, Problem 2)**.** Suppose a finite group G acts on a set A so that for every non-trivial $g \in G$ there exists a unique fixed point (i.e., there is exactly one $a \in A$, depending on g, such that $g(a) = a$). Prove that this fixed point is the same for all $g \in G$.

1.4 Sylow Theory

Lemma 1.4.1. Suppose a p-group G acts on a finite set X, then

$$|X^G| \equiv |X| \pmod{p}.$$

Theorem 1.4.2 (Cauchy)**.** Let G be a group and $p \mid |G|$ be prime, then there exists some $g \in G$ with order p.

Corollary 1.4.3. A p-group G has non-trivial center.

Lemma 1.4.4. Let G be a finite group and $H \subseteq G$ be a p-subgroup, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Theorem 1.4.5 (First Sylow Theorem)**.** Let G be a group of order $p^n \cdot m$ for prime p, $n > 0$, and $\gcd(p, m) = 1$. For $0 \leq k \leq n$, G has a subgroup of order p^k; moreover, for every $0 \leq k \leq n-1$, every subgroup of G of order p^k that is a normal subgroup of a subgroup of order p^{k+1}.

Theorem 1.4.6 (Second Sylow Theorem)**.** Let G be a finite group with order divisible by p, and let $P \subseteq G$ be a Sylow p-subgroup, then

- for every p-subgroup H of G, there exists some $g \in G$ such that $H \subseteq gPg^{-1}$, and
- all Sylow p-subgroups of G are conjuates.

Corollary 1.4.7. A Sylow p-subgroup of G is normal if and only if it is the unique Sylow p-subgroup of G.

Theorem 1.4.8 (Third Sylow Theorem)**.** Let G be a finite group of order $p^n \cdot m$, where p is a prime, $n > 0$, and $\gcd(m, p) = 1$. Then the number of Sylow p-subgroups, denoted n_p, satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.

Proposition 1.4.9. Suppose G is a finite group with a Sylow p-subgroup P, then

- P is the unique Sylow p-subgroup of $N_G(P)$, and
- $N_G(N_G(P)) = N_G(P)$.

Theorem 1.4.10. Let G be a group, then if all Sylow p-subgroups of G are unique (i.e., normal subgroups), then G is the (internal) direct product of all Sylow p-subgroups.

Definition 1.4.11 (Simple)**.** A non-trivial group is simple if it has no non-trivial normal subgroups.

Exercise 1.4.12 (May 2022, Problem 1)**.** (a) Describe all finite groups of order p^2, where p is prime, up to isomorphism.

(b) Describe all finite groups of order 425 up to isomorphism.

Exercise 1.4.13 (January 2021, Problem 1)**.** Let G be a group of order 2057.

(a) Show that $G \cong P \times Q$ where P is a group of order 17 and Q is a group of order 121. Determine all groups of order 2057 up to isomorphism.

(b) Show that $\mathrm{Aut}(G) \cong \mathrm{Aut}(P) \times \mathrm{Aut}(Q)$.

(c) Show that if Q is cyclic, then so is $\mathrm{Aut}(Q)$. What is the order of $\mathrm{Aut}(Q)$ in this case?

(d) If Q is not cyclic, find an isomorphic description of $\mathrm{Aut}(Q)$ and compute its order.

Exercise 1.4.14 (August 2020, Problem 1)**.** (a) A finite group G is called *cool* if G has precisely four Sylow subgroups (over all primes p). The order $|G|$ of a cool group is called a *cool* number. For example, S_3 is a cool group and 6 is a cool number. Describe the set of all cool numbers. Hint: Use prime factorization in your description.

(b) For each cool number n that you found in part (a), determine whether every cool group of order n is nilpotent.

(c) For each cool number n that you found in part (a), determine whether every cool group of order n is solvable.

Exercise 1.4.15 (August 2019, Problem 1)**.** Let p, q be two prime integers. Prove that a group of order p^2q is not simple.

Exercise 1.4.16 (May 2019, Problem 1)**.** Show that any group of order 77 is cyclic.

Exercise 1.4.17 (January 2019, Problem 1)**.** Let G be a p-group. Let H be a normal subgroup of G of order p. Show that H is contained in the center of G.

Exercise 1.4.18 (August 2018, Problem 1)**.** Let G be a finite group of order p^2q^2, with $p \neq q$ prime numbers. Show that there is a Sylow subgroup of G which is normal in G.

Exercise 1.4.19 (May 2018, Problem 1)**.** Let P be a Sylow p-subgroup of a finite group G and let N be a normal subgroup of G, such that $P \cap N \neq \{e\}$. Prove that $P \cap N$ is a Sylow p-subgroup of N.

1.5 Solvable and Nilpotent Groups

Definition 1.5.1 (Commutator Subgroup)**.** Let G be a group and $x, y \in G$, then the commutator of x and y is $[x, y] = xyx^{-1}y^{-1}$. The commutator subgroup of G is $[G, G]$, with elements of the form $[x_1, y_1][x_2, y_2] \cdots [x_n, y_n]$.

Proposition 1.5.2. The commutator subgroup $[G, G]$ is a normal subgroup of G. Moreover, G is abelian if and only if $[G, G]$ is trivial.

Proposition 1.5.3. Let $N \lhd G$ be a normal subgroup, then G/N is an abelian group if and only if $N \supseteq [G, G]$.

Proposition 1.5.4. Let $f : G \to H$ be a group homomorphism to an abelian group H. Let $N \supseteq \ker(f)$ be a subgroup of G, then $N \lhd G$ is a normal subgroup.

Definition 1.5.5 (Subnormal series)**.** A subnormal series of a group G is a series of subgroups $G_0 = G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ such that $G_i \rhd G_{i+1}$ for all i. We usually write

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

Definition 1.5.6 (Normal series)**.** A normal series of a group G is a series of subgroups $G_0 = G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$ such that $G_i \lhd G$ for all i.

Proposition 1.5.7. A normal series is always subnormal.

Definition 1.5.8 (Derived series)**.** A derived series is a series of subgroups $G_0 = G \supseteq G_1 \supseteq G_2 \supseteq \cdots$ where $G_{i+1} = [G_i, G_i]$. In particular, a derived series is a subnormal series.

Definition 1.5.9 (Composition series)**.** A composition series is a subnormal series

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_n = \{e\},$$

that terminates trivially, with all factor groups G_i/G_{i+1} to be simple.

Theorem 1.5.10. Every finite group has a composition series.

Theorem 1.5.11 (Jordan-Hölder)**.** If a group G has a composition series, then any two composition series of G are equivalent, i.e., determines a unique list of simple groups as factors.

Example 1.5.12. $\mathbb{Z}/24\mathbb{Z}$ has the following composition series:

$$(0) \subseteq (8) \subseteq (4) \subseteq (2) \subseteq \mathbb{Z}/24\mathbb{Z},$$

$$(0) \subseteq (12) \subseteq (4) \subseteq (2) \subseteq \mathbb{Z}/24\mathbb{Z},$$

$$(0) \subseteq (12) \subseteq (6) \subseteq (2) \subseteq \mathbb{Z}/24\mathbb{Z},$$

$$(0) \subseteq (12) \subseteq (6) \subseteq (3) \subseteq \mathbb{Z}/24\mathbb{Z}.$$

Definition 1.5.13 (Solvable)**.** Let G be a group, and we define $G_0 = G$, $G_1 = [G, G]$, $G_2 = [G_1, G_1]$, and so on, so G_i/G_{i+1} is always an abelian group. Consider the (subnormal) derived series

$$G = G_0 \rhd G_1 \rhd G_2 \cdots,$$

then we say G is solvable if $G_n = \{e\}$ for some n, that is, the derived series terminates trivially.

Theorem 1.5.14. Given a group G, the following are equivalent:

- G is solvable, i.e, the derived series of G terminates trivially,
- G has a normal series with abelian factor groups,
- G has a subnormal series with abelian factor groups.

Proposition 1.5.15.

- A subgroup of a solvable group is solvable.
- Suppose $N \lhd G$ is a normal subgroup, then G is solvable if and only if N and G/N are both solvable.
- p-groups are solvable.
- If p, q are primes, then a group of order pq has to be solvable.

Definition 1.5.16 (Refinement)**.** Given a subnormal series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$, a subnormal series $G = H_0 \rhd \cdots \rhd H_m$ is a refinement of the subnormal series above if $G_0, G_1, \ldots, G_n$ is a subsequence of $H_0, H_1, \ldots, H_m$.

Theorem 1.5.17. Suppose G is solvable, then it admits a subnormal series with abelian factor groups, then every refinement of such a series is also a subnormal series with abelian factor groups.

Theorem 1.5.18. A subnormal series is a composition series if and only if it has no proper refinements, i.e., every refinement of the series has the same length as the original one.

Theorem 1.5.19 (Schreier)**.** Any two subnormal (respectively, normal) series of a group G have subnormal (respectively, normal) refinements that are equivalent.

Definition 1.5.20 (Central series)**.** A central series is a normal series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

(so $G_i \lhd G$) and such that $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$.

Definition 1.5.21 (Lower central series)**.** A lower central series is a normal series defined by $G_0 = G$, and $G_{i+1} = [G_i, G] \lhd G$.

Definition 1.5.22 (Upper central series)**.** An upper central series is a central series with $G_i/G_{i+1} \cong Z(G/G_{i+1})$.

Remark 1.5.23. Note that if $G_n = \{e\}$, then $G_{n-1} = Z(G)$. Some sources construct the upper central series backwards, that is, with $G_1 = Z(G)$, and define G_i as the unique subgroup of G such that $G_i/G_{i-1} \cong Z(G/G_{i-1})$, then having an upper central series is equivalent to having this series terminates at $G_n = G$ for some n.

Definition 1.5.24 (Nilpotent)**.** A group G is called nilpotent if there exists a normal series of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

(with $G_i \lhd G$) that terminates trivially, and $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$. That is, G has a central series.

Theorem 1.5.25. Given a group G, the following are equivalent:

- G is nilpotent, i.e., G has a central series,
- G has an upper central series,
- G has a lower central series.

Proposition 1.5.26.

- p-groups are nilpotent,
- Abelian groups are nilpotent,
- Finite products of nilpotent groups are nilpotent.
- Nilpotent groups are solvable.
- If $G/Z(G)$ is nilpotent, then so is G.
- If G is nilpotent and $H \subsetneq G$ is a proper subgroup, then $N_G(H) \neq H$.
- Subgroups and quotients of a nilpotent group are nilpotent.

Theorem 1.5.27. A finite group is nilpotent if and only if it is the direct product of its Sylow p-subgroups.

Proposition 1.5.28. A non-trivial nilpotent group has non-trivial center; more generally, every subgroup intersects the center non-trivially.

Exercise 1.5.29 (January 2020, Problem 1)**.** Let G be a finite group of order 100.

(a) Show that G is solvable. (You can use the fact that groups of order p^2 are abelian for p a prime number.)

(b) Show, by giving a counterexample, that G need not be nilpotent.

Exercise 1.5.30 (May 2019, Problem 2)**.** Let q be a prime power and let $\mathbb{F}_q$ be a finite field with q elements. Let $\mathrm{GL}_2(\mathbb{F}_p)$ be the (finite) group of invertible 2×2 matrices with coefficients in $\mathbb{F}_p$.

(a) Show that there is a group homomorphism $\mathrm{GL}_2(\mathbb{F}_q) \to S_{q+1}$ with kernel equal to the subgroup of scalar matrices $Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid 0 \neq a \in \mathbb{F}_q \right\}$. (Hint: construct an action of $\mathrm{GL}_2(\mathbb{F}_q)$ on the set of one-dimensional subspaces of $\mathbb{F}_q^2$.)

(b) Use part (a) to prove that $\mathrm{GL}_2(\mathbb{F}_3)$ is solvable and that $\mathrm{GL}_2(\mathbb{F}_4)$ is not solvable. You may use without proof that $\mathrm{GL}_2(\mathbb{F}_q)$ has cardinality $(q^2-1)(q^2-q)$.

1.6 Symmetric and Alternating Groups

Theorem 1.6.1. S_n is solvable if $n \leq 4$.

Proposition 1.6.2. Every element of S_n is a product of transpositions.

Definition 1.6.3 (Even/Odd permutations)**.** An even permutation is represented as the product of even number of transpositions; an odd permutation is represented as the product of odd number of transpositions.

Definition 1.6.4 (Alternating Group)**.** The alternating group A_n is the subgroup of even permutations of S_n.

Proposition 1.6.5. $A_n \lhd S_n$ is a normal subgroup of index 2.

Example 1.6.6.
- $A_1 \cong S_1 = \{e\}$;
- $A_2 = \{e\}$, $S_2 \cong \mathbb{Z}/2\mathbb{Z}$;
- $A_3 \cong \mathbb{Z}/3\mathbb{Z}$;
- A_4 with order 12 is non-abelian.
- $A_n \subseteq S_n$ is solvable for $n \leq 4$.

Example 1.6.7. For $n \geq 3$, $Z(S_n) = \{e\}$; for $n \geq 4$, $Z(A_n) = \{e\}$.

Corollary 1.6.8. A_n is generated by products of two transpositions for $n \geq 3$.

Lemma 1.6.9. A_n is generated by 3-cycles for $n \geq 3$.

Lemma 1.6.10. For $n \geq 5$, every two 3-cycles in A_n are conjugates.

Proposition 1.6.11.
- An abelian group is simple if and only if it is $\mathbb{Z}/p\mathbb{Z}$ for some prime p.
- A non-abelian simple group is not solvable.

Example 1.6.12. S_3, S_4, A_4 are not simple.

Theorem 1.6.13. A_n is simple for $n \geq 5$.

Corollary 1.6.14. A_n and S_n are not solvable for $n \geq 5$.

Proposition 1.6.15. A_n is the only non-trivial normal subgroup of S_5 if $n \geq 5$.

Exercise 1.6.16 (August 2019, Problem 2)**.** Consider the symmetric group S_n with $n \geq 5$.

(a) Show that any 3-cycle is a commutator.

(b) Let H be a subgroup of S_n and let H_1 be a normal subgroup of H such that H/H_1 is abelian. If H contains all 3-cycles then show that H_1 contains all 3-cycles.

(c) Deduce that S_n is not solvable.

Exercise 1.6.17 (May 2018, Problem 2)**.** Let $\varphi : S_5 \to G$ be a group homomorphism. Classify the image $\varphi(S_5)$, i.e., list all the possibilities for $\varphi(S_5)$ up to isomorphism.

2 Ring Theory

2.1 Additional Structures on Rings

Definition 2.1.1 (Zero Divisor, Integral Domain)**.** A zero divisor is an element $x \in R$ such that there exists $0 \neq y \in R$ such that $xy = 0$.

An integral domain is a commutative ring with cancellation law, or equivalently, has no non-zero zero divisors.

Definition 2.1.2 (Division Ring, Field)**.** A division ring is a ring R with $R^\times = R \setminus \{0\}$, i.e., every non-zero element is invertible.

A field is a commutative division ring.

Theorem 2.1.3 (Chinese Remainder Theorem)**.** Let $I_1, \ldots, I_n$ be ideals in a ring such that $I_k + I + l = R$ for all $k \neq l$, i.e., comaximal. Let $a_1, \ldots, a_n \in R$, then there exists some $a \in R$ such that $a \equiv a_i \pmod{I_i}$ for all i, i.e., $a - a_i \in I_i$ for all i.

Definition 2.1.4 (Prime Ideal)**.** A prime ideal $P \subseteq R$ of a commutative ring is an ideal such that $P \neq R$ and whenever $xy \in P$, either $x \in P$ or $y \in P$.

Proposition 2.1.5. An ideal $P \subseteq R$ of a commutative ring is a prime ideal if and only if R/P is an integral domain.

Definition 2.1.6 (Maximal Ideal)**.** A maximal ideal $M \subseteq R$ of a commutative ring is an ideal where $M \neq R$, and whenever $M \subseteq M' \subseteq R$ for some ideal M' of R, then $M' = M$ or $M' = R$.

Proposition 2.1.7. An ideal $M \subseteq R$ of a commutative ring is maximal if and only if R/M is a field.

Corollary 2.1.8. A maximal ideal is a prime ideal.

Proposition 2.1.9. A commutative ring R has exactly two ideals if and only if R is a field.

Lemma 2.1.10 (Zorn)**.** Every non-trivial ring has a maximal ideal.

Exercise 2.1.11 (January 2020, Problem 2)**.** Decide which of the following sets are ideals of the ring $\mathbb{Z}[x]$. Provide justification.

(a) The set of all polynomials whose coefficient of x^2 is a multiple of 3.

(b) $\mathbb{Z}[x^2]$, the set of all polynomials in which only even powers of x appear.

(c) The set of polynomials whose coefficients sum to zero.

Exercise 2.1.12 (August 2018, Problem 2)**.** Let R be a ring with identity 1. An element $x \in R$ is called *nilpotent* if $x^n = 0$ for some positive integer n. Denote by $N \subseteq R$ the set of nilpotent elements. Show that:

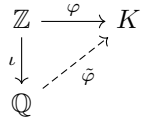
(a) if x is nilpotent, then $1 - x$ is a unit;

(b) if R is commutative, then $N \subseteq R$ is an ideal;

(c) if R is commutative, then R/N has exactly one nilpotent element.

Exercise 2.1.13 (January 2021, Problem 2)**.** Let R be the ring of 3×3 matrices over $\mathbb{Q}$, and S denote the ring of 2×2 matrices over $\mathbb{Q}$. Is there a surjective ring homomorphism $\varphi : R \to S$?

Exercise 2.1.14 (January 2021, Problem 4)**.** Let K be a field. Define the ring homomorphism $\varphi : \mathbb{Z} \to K$ by $\varphi(n) = n \cdot 1$. If φ is injective and $\iota : \mathbb{Z} \to \mathbb{Q}$ is the standard inclusion, prove that there exists an injective ring homomorphism $\tilde{\varphi} : \mathbb{Q} \to K$ such that the diagram



is commutative.

2.2 Integral Domains and Factorizations

Throughout this section, R is an integral domain.

Definition 2.2.1 (PID)**.** An integral domain R is a principal ideal domain (PID) if every ideal of R is principal, i.e., can be generated by one element in R.

Definition 2.2.2 (Euclidean Domain)**.** A integral domain R is a Euclidean domain if there exists some function $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for every $a, b \in R$ and $a \neq 0$, there exists some $q, r \in R$ such that $b = aq + r$ for either $r = 0$ or $\varphi(r) < \varphi(a)$.

Theorem 2.2.3. Every Euclidean domain is a PID.

Example 2.2.4.

- $\mathbb{Z}$ is Euclidean with $\varphi(a) = |a|$.
- The polynomial ring $F[x]$ over a field F is Euclidean with $\varphi(f) = \deg(f) \geq 0$.
- The Gaussian integers $\mathbb{Z}[i]$ is Euclidean with $\varphi(a + bi) = a^2 + b^2$.

Example 2.2.5. Although a quadratic extension of $\mathbb{Z}$, as an integral domain $\mathbb{Z}[\sqrt{n}]$ for some $n \in \mathbb{Z}$, is not Euclidean, it still has a norm function $N(a + b\sqrt{n}) = a^2 - nb^2$. Note that this may not be a Euclidean function since the image may land in negative integers.

A norm has to be an integer, and it is ± 1 if and only if $a + b\sqrt{n}$ is a unit.

Definition 2.2.6 (Prime)**.** An element $p \in R$ is said to be prime if p is non-zero, non-unit, and $p \mid ab$ in R implies $p \mid a$ or $p \mid b$.

Proposition 2.2.7. $p \in R$ is prime if and only if $(p) \subseteq R$ is a prime ideal.

Definition 2.2.8 (Irreducible)**.** An element $c \in R$ is said to be irreducible if c is non-zero, non-unit, and $c = ab$ implies $a \in R^\times$ or $b \in R^\times$.

Proposition 2.2.9. Every prime element is irreducible.

Definition 2.2.10 (Factorization, UFD)**.** An integral domain R admits a factorization if every non-zero non-unit element can be written as a product of irreducible elements.

A unique factorization domain (UFD) is an integral domain with a unique factorization.

Proposition 2.2.11. In a UFD R, irreducible elements are prime. In particular, they are equivalent.

Theorem 2.2.12. An integral domain R is a UFD if and only if R admits a factorization, and the prime elements and irreducible elements are equivalent.

Corollary 2.2.13. A PID is a UFD.

Remark 2.2.14. For an integral domain R, R being Euclidean implies R being a PID, implies R being a UFD.

Exercise 2.2.15 (May 2019, Problem 4)**.** Let k be a field, and consider the element $D = \det \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ in the polynomial ring $k[x, y, z, w]$.

(a) Show that D is irreducible.

(b) Show that $k[x, y, z, w]/D$ is not a UFD.

Exercise 2.2.16 (January 2019, Problem 3)**.** (a) Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

(b) Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. Show that the ideal $I = (3, 2 + \sqrt{-5})$ is not principal.

(c) Is it possible for R, as defined in part (b), to be a Euclidean domain with respect to some norm?

Definition 2.2.17 (Greatest Common Divisor)**.** Let R be a UFD and $a_1, \ldots, a_n$ be non-zero elements, then consider the unique factorization of distinct irreducible elements $c_1, \ldots, c_m$ such that $a_i = \prod_{j=1}^{m} c_j^{k_{ij}}$ for each i up to multiplication of units. The greatest common divisor of $a_1, \ldots, a_n$ is the ideal given by $\prod_{j=1}^{m} c_j^{s_j}$ where $s_j = \min_i(k_{ij})$.

Proposition 2.2.18. If R is a UFD, then the greatest common divisor exists, and is unique up to multiplication of units.

Remark 2.2.19. To find the greatest common divisor of two elements in a Euclidean domain (for instance, the Gaussian integers $\mathbb{Z}[i]$), we can use Euclidean algorithm, where each time we find the element closest to the quotient on the lattice of Gaussian integers. The algorithm ends when we no longer attains a remainder.

Exercise 2.2.20 (January 2021, Problem 2)**.** Compute $\gcd(17 + i, 24 + 2i)$ in the ring $\mathbb{Z}[i]$.

Exercise 2.2.21 (August 2020, Problem 3)**.** Compute, if possible, $\gcd(2+8i, 17-17i)$ in the ring $\mathbb{Z}[i]$ of Gaussian integers.

2.3 Polynomial Rings and Irreducibility

Proposition 2.3.1. Suppose F is a field, then $F[x]$ is a PID.

Definition 2.3.2 (Content, Primitive)**.** Let R be a UFD, the content of non-zero polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ is $C(f) = \gcd(a_0, \ldots, a_n)$. In particular, $f(x)$ is primitive if $C(f)$ is a unit.

Proposition 2.3.3. If f is a monic polynomial, then f is primitive. Moreover, $C(af) = aC(f)$ for $0 \neq a \in R$ and $0 \neq f(x) \in R[x]$.

Lemma 2.3.4 (Gauss)**.** If R is a UFD, and $f, g \in R[x]$ are primitive, then fg is primitive as well.

Corollary 2.3.5. $C(fg) = C(f) \cdot C(g)$.

Lemma 2.3.6. Let f and g be non-zero polynomials in $R[x]$ where g is primitive. Let F be the field of fractions of R, then if $g \mid f$ in $F[x]$, then $g \mid f$ in $R[x]$.

Lemma 2.3.7. Let R be a UFD, then an irreducible polynomial $f(x) \in R[x]$ is primitive.

Lemma 2.3.8. Let R be a UFD and let $f(x) \in R[x]$ be a non-constant polynomial. Then f is irreducible in $R[x]$ if and only if f is primitive and irreducible in $F[x]$.

Theorem 2.3.9. If R is UFD, then so is $R[x]$.

Theorem 2.3.10. Let R be a UFD with field of fractions F. Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$. Suppose there exists some irreducible element $p \in R$ such that

- $p \nmid a_n$,
- $p \mid a_i$ for $i = 0, \ldots, n-1$, and
- $p^2 \nmid a_0$,

then f is irreducible in $F[x]$.

Corollary 2.3.11. Let $R = \mathbb{Z}$ and $F = \mathbb{Q}$, then this holds for the usual polynomials. One can also take $R = \mathbb{Z}[i]$ and $F = \mathbb{Q}[i]$, for instance.

Theorem 2.3.12 (Rational Root Theorem)**.** Given a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, any rational root must be of the form $\frac{p}{q}$ where $p \mid a_0$ and $q \mid a_n$ (with possibly negative signs).

Theorem 2.3.13. If $f(x) \in \mathbb{Z}[x]$ is irreducible over some field $\mathbb{F}_p$ for some prime p, then $f(x)$ is irreducible over $\mathbb{Z}$. Conversely, if $f(x) \in \mathbb{Z}[x]$ attains a degree-n factor in $\mathbb{Z}[x]$, then this degree-n factor must descend to $\mathbb{F}_p$ for every prime p, possibly can be further decomposed.

Theorem 2.3.14 (Newton Polygon)**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and p be a prime. The Newton polygon is the lowest convex hull on the scatter plot with points $(i, \nu(i))$ to illustrate that the coefficient a_i on degree i has $p^{\nu(i)} \mid a_i$ but $p^{\nu(i)+1} \nmid a_i$.

If f is monic with Newton polygon given by one line segment of slope $-\frac{c}{n}$, i.e, $\nu(n) = 0$ and $\nu(0) = c$, such that $\gcd(c, n) = 1$, then f is irreducible over $\mathbb{Q}_p$ (p-adic), therefore irreducible in $\mathbb{Q}$.

Proposition 2.3.15. If a polynomial $f(x) \in R[x]$ of degree of degree 2 or 3 does not have a root in R, then $f(x)$ is irreducible.

Exercise 2.3.16 (May 2022, Problem 3)**.** Completely factor the following polynomials over the given fields, or prove they are irreducible.

(a) $x^3 + x + 2 \in \mathbb{Z}_3[x]$.

(b) $x^4 + x^3 + x + 3 \in \mathbb{Z}_5[x]$.

(c) $x^4 + x^3 + x^2 + 6x + 1 \in \mathbb{Q}[x]$.

Exercise 2.3.17 (August 2021, Problem 2)**.** (a) Show that $x^6 + 69x^5 - 511x + 363$ is irreducible over the integers.

(b) Show that $x^4 + 5x + 1$ is irreducible over the rationals.

(c) Show that $x^4 + x^3 + x^2 + 6x + 1$ is irreducible over the rationals.

(d) Calculate the number of distinct, irreducible polynomials over $\mathbb{Z}_5$ that have the form

$$f(x) = x^2 + ax + b, \quad \text{or} \quad g(x) = x^3 + \alpha x^2 + \beta x + \gamma, \quad a, b, \alpha, \beta, \gamma \in \mathbb{Z}_5.$$

Exercise 2.3.18 (August 2020, Problem 3)**.** Determine whether the following polynomials are reducible or irreducible in given rings:

- $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$, where $\mathbb{Z}_2$ is the field of two elements;
- $x^4 + 5x^3 + 10x^2 + 15x + 5$ in $R[x]$, where $R = \mathbb{Z}[i]$;
- $2x^4 + 4x^3 + 8x^2 + 12x + 20$ in $\mathbb{Z}[x]$.

Exercise 2.3.19 (January 2020, Problem 4)**.** Determine if the following polynomials are irreducible over $\mathbb{Z}$.

(a) $x^3 - 5x - 1$,

(b) $x^4 + 10x^2 + 5$.

3 Module Theory

3.1 Free and Torsion Modules

Definition 3.1.1 (Free, Projective)**.** Let M be an R-module, then M is free if M has an R-basis, i.e., every element of M can be written as a unique R-linear combination where almost all coefficients are zero.

An R-module M is projective if it is a direct summand of some free R-module.

Proposition 3.1.2. A free R-module is a projective R-module.

Definition 3.1.3 (Torsion, Torsion-free)**.** Let R be a domain and M be an R-module. An element $m \in M$ is torsion if there exists some non-zero element $a \in R$ such that $am = 0$.

An R-module M is torsion if all elements are torsion. An R-module M is torsion-free if the only torsion element is 0.

Lemma 3.1.4. The torsion subset N of a module M is a submodule of M. Moreover, M/N is torsion-free.

Theorem 3.1.5. A finitely-generated torsion-free module over a PID is free.

Exercise 3.1.6 (May 2018, Problem 4)**.** Let $\langle(11, 13)\rangle$ be the subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ generated by the element $(11, 13)$. Show that the quotient group $(\mathbb{Z} \oplus \mathbb{Z})/\langle(11, 13)\rangle$ is torsion-free.

3.2 Elementary Divisors, Invariant Factors, Structure Theorem

For the rest of the section, let R be a PID.

Definition 3.2.1 (Primary)**.** Let M be a torsion, finitely-generated R-module, let $0 \neq P \subseteq R$ be a non-zero prime ideal of R, then $P = (p)$ for some $p \in P$. An element $m \in M$ is P-primary if $P^n \cdot m$, i.e., $p^n m = 0$ for some $n > 0$.

The set of P-primary elements in M, denoted $M(P)$, is a submodule of M.

Theorem 3.2.2. Every finitely-generated P-primary R-module M is isomorphic to a direct sum of cyclic R-modules R/P^k.

Remark 3.2.3. In particular, $M \cong R^n \oplus N$ where N is the torsion submodule of M. Here N is a finite direct sum of $M(P)$'s, therefore it is a direct sum of cyclic modules.

Therefore, suppose M is a torsion R-module where R is a PID. There should exist distinct prime ideals $P_1, \ldots, P_k$ such that

$$M \cong \bigoplus_{1 \leq i \leq k} \bigoplus_{1 \leq j \leq t_i} R/P_i^{\alpha_{ij}}.$$

Without loss of generality, say $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{it_i}$ for all i.

Definition 3.2.4 (Elementary Divisor)**.** The family of prime ideals $\{P_i^{ij}\}$ is called the set of elementary divisors of M, which is unique up to permutation of terms.

Definition 3.2.5 (Invariant Factors)**.** By the Chinese Remainder Theorem, let $I_j = \prod_{i=1}^{k} P_i^{\alpha_{ij}}$ for each j, then we have

$$R/I_j \cong \prod_{i=1}^{k} (R/P_i^{\alpha_{ij}}).$$

So the torsion module $M \cong \bigoplus_{i=1}^{s} R/I_i$ where $s = \max_{1 \leq i \leq k} t_i$. In particular, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_s$. Since R is a PID, if we say $I_i = (a_i)$, then we have $a_s \mid a_{s-1} \mid \cdots \mid a_2 \mid a_1$. The set of a_i's are called the invariant factors, which is unique up to multiplication choice of generators.

Remark 3.2.6. Let M be a finitely-generated R-module, then it is a factor moodule of some finitely-generated free R-module F, and there exists some submodule $N \subseteq F$ such that $M \cong F/N$. Note that N is free. Let $\{x_1, \ldots, x_n\}$ be a basis of F and let $\{y_1, \ldots, y_m\}$ be a basis of N with $n \geq m$. Since $N \subseteq F$, for every $1 \leq j \leq m$ we have $y_j = \sum_{i=1}^{n} a_{ij} x_j$. We must the linear combination of y_i into the ith column of a matrix, then we have a matrix

$$A = (a_{ij}).$$

(Note that the matrix is the transpose of the linear system above.) By the elementary row/column operations, including

- transposition of two rows, which does not change M, N, or F;
- subtraction from a row (respectively, column) an R-multiple of another row (respectively, column), which changes the basis elements, but not the modules themselves;
- multiplication of a row/column by a unit of R, which does not change the modules.

In particular, A can be transformed into a new matrix with entries on the main diagonal as $(a_{ii}) = (t_1, \ldots, t_k, 0, \ldots, 0)$. In particular, $t_i \neq 0$ for all i, and $t_1 \mid t_2 \mid \cdots \mid t_k$, then this gives $M \cong R/t_1R \oplus R/t_2R \oplus \cdots \oplus R/t_kR \oplus R \oplus \cdots \oplus R$, where there are $m - k$ terms of R-summands. The invariant factors of M are just the invariant factors of the torsion submodule of M, namely $t_1, \ldots, t_k$.

For $R = \mathbb{Z}$, we obtain the structure theorem.

Theorem 3.2.7 (Structure Theorem)**.** Every finitely-generated abelian group is isomorphic to a direct sum of cyclic groups, either $\mathbb{Z}$ or $\mathbb{Z}/p^n\mathbb{Z}$ for some prime p. Two groups are isomorphic if and only if they have the same rank and the same elementary divisors.

Every finitely-generated abelian group is isomorphic to a direct sum of the form $\mathbb{Z}^m \oplus \mathbb{Z}/a_1\mathbb{Z} \cdots \mathbb{Z}/a_s\mathbb{Z}$ with $a_1 \mid \cdots \mid a_s$, where the ideals $a_1\mathbb{Z}, \ldots, a_s\mathbb{Z}$ are uniquely determined. Two groups are isomorphic if and only if they have the same rank and the same invariant factors.

Exercise 3.2.8 (May 2019, Problem 3)**.** Let M be the quotient abelian group $\mathbb{Z}^4/A$, where A is the subgroup of $\mathbb{Z}^4$ generated by the elements $(1, 1, 1, 1)$, $(0, 1, 1, 0)$, and $(1, 2, -1, 0)$.

(a) Determine the structure of M.

(b) How many non-trivial homomorphisms $M \to \mathbb{Z}/5\mathbb{Z}$ are there?

Exercise 3.2.9 (January 2019, Problem 2)**.** Find all abelian groups, up to isomorphism, of order 360 by listing in each case the elementary divisors and the corresponding invariant factors.

3.3 Jordan Canonical Forms and Rational Canonical Forms of Linear Operators

Let F be a field, V be a finite-dimensional F-vector space, and let $S : V \to V$ be a linear operator. One can view V to be a F-module, then S is a V-endomorphism.

In particular, let $R = F[x]$, then R is a PID. There is now a correspondence between

- torsion finitely-generated R-module V,
- linear operator on V defined by $S(v) = x \cdot v$, and
- the square matrix form of linear operator $[S]_B$ with respect to some basis B.

In this sense, the direct sum $V \oplus W$ of modules corresponds to the direct sum of operators $S_1 \oplus S_2 : V \oplus W \to V \oplus W$ and to the square matrix with diagonal blocks of each summand given by $[S_1 \oplus S_2]_{B_1 \cup B_2} = \mathrm{diag}([S_1]_{B_1}, [S_1]_{B_2})$.

Since we know the modules are given by cyclic summands by the structure theorem, so we will look at the cyclic correspondence in particular.

Without loss of generality, let $f(x) = x^n + a_{n-1}x^n + \cdots + a_1 x + a_0 \in F[x]$ be a monic polynomial, then there is a canonical map $R = F[x] \twoheadrightarrow M = R/fR$ via $g \mapsto \bar{g}$ by modulo $f(x)$. Now $\{\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}\}$ becomes a basis of $M = R/fR$, so $S : M \to M$ is the operator $S(\bar{g}) = x \cdot \bar{g}$. Therefore, $S(\bar{x}^i) = \bar{x}^{i+1}$ for $i < n-1$, and $S(\bar{x}^{n-1}) = \bar{x}^n = -a_0 \cdot \bar{1} - a_1 \cdot \bar{x} - \cdots - a_{n-1} \cdot \bar{x}^{n-1}$. Therefore, this corresponds to the matrix $[S]_B$ of the form

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Definition 3.3.1 (Companion Matrix)**.** The cyclic correspondence above gives a connection between cyclic R-module R/fR, cyclic operator $S : V \to V$, and the matrix $[S]_B$ above. In particular, we call the matrix above the companion matrix $C(f)$ of f.

Theorem 3.3.2. Let V be a finite-dimensional F-vector space and $S : V \to V$ be a linear operator, then

- there exists unique monic polynomials $f_1 \mid f_2 \mid \cdots \mid f_r$ such that the matrix of S in some basis is the block diagonal matrix of the form $\mathrm{diag}(C(f_1), \ldots, C(f_r))$. This is the canonical form of S.
- there exists unique (up to permutations) polynomials $p_1^{k_1}, \ldots, p_s^{k_s}$ where p_i's are monic irreducible polynomials, such that the matrix of S in some basis is the block diagonal matrix $\mathrm{diag}(C(p_1^{k_1}), \ldots, C(p_s^{k_s}))$.

Theorem 3.3.3. Let A be an $n \times n$ matrix over a field F, then

- there exists unique monic polynomials $f_1 \mid f_2 \mid \cdots \mid f_r$ such that A is similar to $\mathrm{diag}(C(f_1), \ldots, C(f_r))$.
- there exists unique (up to permutations) polynomials $p_1^{k_1}, \ldots, p_s^{k_s}$ where p_i's are monic irreducible polynomials, such that the A is similar to the block diagonal matrix $\mathrm{diag}(C(p_1^{k_1}), \ldots, C(p_s^{k_s}))$.

Definition 3.3.4 (Rational Canonical Form)**.** The rational canonical form (RCF) of a square matrix A is the diagonal block matrix $\mathrm{diag}(C(f_1), \ldots, C(f_r))$, where each $C(f_i)$ is the companion matrix of invariant factor f_i.

To find the RCF of a matrix A, we know correspondingly there is the matrix $x \cdot I_n - A$ over $R = F[x]$.

Definition 3.3.5 (Characteristic Polynomial)**.** The characteristic polynomial of square matrix A is the determinant $p_A(x) = \det(x \cdot I_n - A)$, which is monic of degree n.

Proposition 3.3.6. $p_A(x) = \prod_{i=1}^{r} f_i$, i.e., the characteristic polynomial is the product of all invariant factors.

Now consider the submodule $N \subseteq R^n$ generated by the columns of $x \cdot I_n - A$.

Lemma 3.3.7. $\dim_F(R^n/N) = n$.

Therefore, after choosing a basis $\{v_1, \ldots, v_n\}$ for V, we define the R-module homomorphism with respect to the linear operator S on V by

$$g : R^n \to V$$

$$(f_1, \dots, f_n) \mapsto \sum_{i=1}^{n} f_i(S)(v_i).$$

Remark 3.3.8. For instance, if we look at the $\mathbb{C}[x]$-module structure of an $n \times n$ matrix A with entries in $\mathbb{C}$, then this is given by an R-module homomorphism $\mathbb{C}^n \to R = \mathbb{C}[x]$ defined by $f(x) \cdot v = f(A) \cdot v$ for $v \in \mathbb{C}^3$. Therefore, $\mathbb{C}^n$ now has the structure as a $\mathbb{C}[x]$-module by the factorization.

To find the invariant factors of V, we need to find the invariant factors of R^n/N, then we calculate the decomposition after choosing a basis. Note that some polynomials in the decomposition may be units, and we need to omit them. The invariant factors are the non-units of this factorization.

Example 3.3.9. Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$, then we have $x \cdot I_2 - A = \begin{pmatrix} x & 2 \\ -1 & x-3 \end{pmatrix}$, now interchanging the rows with multiplication of units give

$$\begin{pmatrix} 1 & 3-x \\ x & 2 \end{pmatrix}$$

and subtracting the first row multiplied by x from the second row gives

$$\begin{pmatrix} 1 & 3-x \\ 0 & x^2-3x+2 \end{pmatrix},$$

and finally subtracting the first column multiplied by $3-x$ from the second column gives

$$\begin{pmatrix} 1 & 0 \\ 0 & x^2-3x+2 \end{pmatrix}.$$

Since 1 is a unit, then the only invariant factor is x^2-3x+2. This agrees with the companion matrix $C(x^2-3x+2) = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$.

Definition 3.3.10 (Minimal polynomial)**.** Consider the annihilators of V, namely the set $\{f \in R : f \cdot V = 0\}$, i.e., $f(S)(V) = 0$. Since this is an ideal, then it can be generated by one element $0 \neq f_{\min} \cdot R$, which is monic. We say $f_{\min}$ is the minimal polynomial of $S : V \to V$.

Note that $f_{\min} \cdot V = 0$, and it is the smallest element annihilating V. Therefore, looking at the invariant factors, we see $V = \bigoplus_{i=1}^{s} R/f_iR$, then $\operatorname{Ann}(R/f_iR) = f_iR$, so since f_s is divisible by all other invariant factors, then by definition we have $f_{\min} = f_s$.

Proposition 3.3.11. The minimal polynomial of the linear operator is the largest invariant factor. This does not depend on the base field.

Corollary 3.3.12. The minimal polynomial divides the characteristic polynomial.

Corollary 3.3.13. Let A and B be matrices over F, and let $L \supseteq F$, then $A \sim B$ are similar matrices over F if and only if $A \sim B$ are similar matrices over L.

Recall that the roots of the characteristic polynomial are just the eigenvalues of the matrix (counted with multiplicities).

Proposition 3.3.14. Given a vector space V over F and a corresponding matrix A, the following are equivalent:

- A is diagonalizable,

- there exists an eigenbasis, i.e., basis of eigenvectors,
- V is a direct sum of all eigenspaces, i.e., the space of eigenvectors corresponding to an eigenvalue λ,
- all elementary divisors of A are linear,
- all invariant factors of A are products of distinct linear polynomials,
- the minimal polynomial is a product of distinct lineaer polynomials.

In particular, the characteristic polynomial splits as a product of linear factors.

Proposition 3.3.15. Similarly, with the same assumption, the following are equivalent:

- V is cyclic,
- the set of invariant factors if a singleton,
- the minimal polynomial equials the characteristic polynomial,
- all elementary divisors are pairwise relatively prime.

Now let $S : V \to V$ be a linear operator and assume that the characteristic polynomial splits. Therefore, we have $p_S(x) = \prod_{i=1}^{n}(x - \lambda_i)$ where $n = \dim(V)$ and λ_i's are the eigenvalues. In particular, every elementary divisor has the form $(x - \lambda_i)^k$ for some i. We want to find a basis for the cyclic summand $M_i = R/(x - \lambda_i)^k R$. There is an obvious basis of $\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{k-1}$, then by a change of variables $y = x - \lambda$, we have a new basis of $1, x - \lambda, \ldots, (x - \lambda)^{k-1}$. The matrix with respect to this basis is of the form

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

We denote this matrix by $J(\lambda_i, k)$, as the $k \times k$ matrix with respect to the eigenvalue λ. This is called a Jordan block.

Definition 3.3.16 (Jordan Canonical Form)**.** Let $S : V \to V$ be a linear operator in a finite-dimensional vector space V. Suppose the characteristic polynomial splits, then there exists some basis of V such that the matrix of S is a diagonal block matrix of the form $\mathrm{diag}(J(\lambda_1, k_1), \ldots, J(\lambda_s, k_s))$, possibly with repetition, but is determined uniquely up to permutations. This diagonal block matrix is called the Jordan canonical form of S.

Remark 3.3.17. Given an $n \times n$ matrix M over a field F with an eigenvalue λ, and suppose the F-dimension of the nullspace of $\lambda \cdot \mathrm{id} - M$ is m. Denote this space by $N(A^1)$ of dimension N_1, where $A = \lambda \cdot \mathrm{id} - M$ is the matrix with entries below diagonal as 1's. Therefore, the number of Jordan blocks with eigenvalue λ is just m. This actually gives $N_1 = n - \dim(A^1) = \dim(N(A^1))$. Proceeding inductively, we have $N_i = n - \dim(A^i) = \dim(N(A^i))$, and this corresponds to the number of Jordan blocks with size at least i. Therefore, if we are given the dimension of nullspaces $N_i = \dim(N(A^i))$, then each time $N_k - N_{k-1}$ is the number of Jordan blocks with size at least k.

Example 3.3.18. Suppose we have M to be a 12×12 matrix with one eigenvalue λ. Suppose $\dim(N(\lambda \cdot I - M)) = 4$, $\dim(N(\lambda \cdot I - M)^2) = 7$, and $\dim(N(\lambda \cdot I - M)^3) = 10$, and $\dim(N(\lambda \cdot I - M)^4) = 12$, then there are four Jordan blocks (with size at least 1), $7 - 4 = 3$ Jordan blocks with size at least 2, $10 - 7 = 3$ Jordan blocks with size at least 3, and $12 - 10 = 2$ Jordan blocks with size at least 4. Therefore, this means we have four Jordan blocks, with size 4, 4, 3, 1.

Example 3.3.19. Suppose we have $M = \operatorname{diag}(J(\lambda,2), J(\lambda,2), J(\lambda,3), J(\lambda,4), J(\lambda,4))$ as a 15×15 matrix, then the rank of each Jordan block $J(\lambda, i)$ is the dimension $i-1$ (since there are 1's below the diagonal). Therefore, the total dimension is $(2-1)+(2-1)+(3-1)+(4-1)+(4-1) = 10$. By rank-nullity theorem, the nullity is $15-10=5$, but we note that each Jordan block only contributes to nullity by dimension 1, namely given by the first element of the column vector, so the total number of Jordan blocks must be 5, given by the nullity of $\lambda \cdot I - M$. This shows that the number of Jordan blocks with size at least k is the nullity of $(\lambda \cdot I - M)^k$, namely the dimension $\dim((\lambda \cdot I - M)^{k-1}) - \dim((\lambda \cdot I - M)^k)$.

Exercise 3.3.20 (May 2022, Problem 2)**.** Make $\mathbb{C}^3$ into a $\mathbb{C}[x]$-module by $f(x)v = f(A)v$ where $v \in \mathbb{C}^3$ and

$$A = \begin{pmatrix} 5 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 3 & 3 \end{pmatrix}.$$

Find polynomials $p_i(x)$ and exponents e_i such that $\mathbb{C}^3 \cong \bigoplus_i \mathbb{C}[x]/(p_i^{e_i})$ as $\mathbb{C}[x]$-modules.

Exercise 3.3.21 (August 2021, Problem 3)**.** Find possible Jordan canonical forms of an 8×8 matrix M over the field $\mathbb{F}_5$ with five elements if it is known that the characteristic polynomial of M is $(x^2+1)^4$ and the minimal polynomial of M is $(x^2+1)^2(x+2)$.

Exercise 3.3.22 (January 2021, Problem 3)**.** Suppose A is a 9×9 matrix over the field $\mathbb{F}_5$ with 5 elements such that the characteristic polynomial of A is $(x-1)^2(x-3)^4(x^3-1)$ and the minimal polynomial of A is $(x-1)(x-3)^3(x^3-1)$. Compute the following:

(a) The possible Jordan canonical form (or forms) of A over a suitable extension of $\mathbb{F}_5$;

(b) The possible rational canonical form (or forms) of A.

Exercise 3.3.23 (August 2020, Problem 4)**.** Let A be an $n \times n$ complex matrix and let f and g be the characteristic and minimal polynomials of A, respectively. Suppose that $f(x) = g(x)(x-i)$ and $g(x)^2 = f(x)(x^2+1)$. Determine all possible Jordan canonical forms of A.

Exercise 3.3.24 (January 2020, Problem 3)**.** Find the possible Jordan canonical forms of 7×7 matrices M with entries in $\mathbb{C}$ satisfying the following criteria:

- the characteristic polynomial of M is $(z-3)^4(z-5)^3$,
- the minimal polynomial of M is $(z-3)^2(z-5)^2$, and
- the $\mathbb{C}$-vector space dimension of the nullspace of $3 \cdot \mathrm{id} - M$ is 2.

Exercise 3.3.25 (August 2019, Problem 3)**.** Let V be a finite-dimensional real vector space and $\varphi : V \to V$ a linear transformation with invariant factors $q_1 = x^4 - 4x^3 + 5x^2 - 4x + 4 = (x-2)^2(x^2+1)$ and $q_2 = x^7 + 6x^6 + 14x^5 - 20x^4 + 25x^3 - 22x^2 + 12x - 8 = (x-2)^3(x^2+1)^2$ in $\mathbb{R}[x]$.

(a) Find the rational canonical form of φ with respect to some basis.

(b) Suppose V is a complex vector space and $\psi : V \to V$ is a linear transformation with same invariant factors as above.

(i) Find the elementary divisors of ψ in $\mathbb{C}[x]$.

(ii) Find the Jordan canonical form of ψ with respect to some basis.

Exercise 3.3.26 (August 2018, Problem 3)**.** Let V denote the vector space over $\mathbb{R}$ of real polynomials of degree $\leq n$. Let $T : V \to V$ be the linear map given by $T(p(x)) = p'(x)$.

(a) Find the Jordan canonical form of T.

(b) Find the rational canonical form of T.

Exercise 3.3.27 (May 2018, Problem 3)**.** Let $T : \mathbb{Q}^4 \to \mathbb{Q}^4$ be the $\mathbb{Q}$-linear transformation which relative to some basis is represented by the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}.$$

Find the rational canonical form for T.

4 Galois Theory

4.1 Algebraic Extensions

Proposition 4.1.1. Every field homomorphism is injective.

Definition 4.1.2 (Field Extension, Degree)**.** Let $F \subseteq K$ be a subfield, we say K is an extension of F and denote K/F. We denote $[K : F] = \dim_F(K)$ to be the degree of K over F.

Proposition 4.1.3. Let $L/K/F$ be a field tower extension, then $[L : F] = [L : K] \times [K : F]$. In particular, $[L : F]$ is finite if and only if $[L : K]$ and $[K : F]$ are finite.

Definition 4.1.4 (Generated Field)**.** Let K/F be a field extension and $S \subseteq K$ be a subset, then there is a unique smallest subfield of K containing S, given by the intersection of all subfield of K containing S. Consider $T = S \cup F$, then we denote $F(S)$ to be the smallest subfield of K containing T. Note that $K/F(S)/F$ is a field tower, so $F(S)$ is the smallest subfield of K containing F and S, called the field generated by T over K.

Lemma 4.1.5. Let K/F be a field extension and let $\alpha_1, \ldots, \alpha_n \in K$. Then $F(\alpha_1, \ldots, \alpha_n)$ is the set of fractions $\frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n}$ where $f(\alpha_1, \ldots, \alpha_n), g(\alpha_1, \ldots, \alpha_n \in F[x_1, \ldots, x_n]$ and $g(\alpha_1, \ldots, \alpha_n) \neq 0$.

Definition 4.1.6. Let K/F be a field extension and let $\alpha_1, \ldots, \alpha_n \in K$, then $F[\alpha_1, \ldots, \alpha_n]$ is the ring of polynomials $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$.

Remark 4.1.7. $F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n)$ if and only if $F[\alpha_1, \ldots, \alpha_n]$ is a field.

Definition 4.1.8 (Algebraic Transcendental)**.** Suppose K/F is a field extension, then we say $\alpha \in F$ is algebraic over F if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. If α is not algebraic, then α is called transcendental over F.

We say K/F is an algebraic extension if every $\alpha \in K$ is algebraic over F.

Proposition 4.1.9. Let K/F be a field extension.

- $\alpha \in F$ is algebraic.
- Suppose $\alpha \in L$ where $L/K/F$ is a tower of extensions. If α is algebraic over F, then α is algebraic over K.
- If $\alpha \in K$ is transcendental over F, then $F[\alpha] \cong F[x]$ by an isomorphism

$$\begin{aligned} F[x] &\to F[\alpha] \\ g &\mapsto g(\alpha) \end{aligned}$$

  Moreover, $F(x) \cong F(\alpha)$.
- $x \in F(x)$ is transcendental over F.

Theorem 4.1.10 (Minimal polynomial)**.** Let $\alpha \in K/F$ be algebraic over F, then

- there exists a unique monic irreducible polynomial $m_\alpha \in F[x]$ such that $m_\alpha(\alpha) = 0$;
- if $f(\alpha) = 0$ for $f \in F[x]$, then $m_\alpha \mid f$;
- the elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ where $n = \deg(m_\alpha)$ give a basis for the extension $F(\alpha)$ over F. In particular, we have $[F(\alpha) : F] = \deg(m_\alpha)$;

- $F(\alpha) = F[\alpha]$. In particular, this holds if and only if α is algebraic.

Example 4.1.11 (Cyclotomic Polynomial)**.** Let p be a prime integer, and denote $\zeta_p = \cos\left(\frac{2\pi}{p}\right) + i \cdot \sin\left(\frac{2\pi}{p}\right)$, where $(\zeta_p)^p = 1$ and $\zeta_p \neq 1$. In particular, ζ_p is a root of $x^p - 1$, therefore it is a root of $x^{p-1+\cdots+x+1}$. In particular, this is the minimal polynomial of ζ_p, with $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Corollary 4.1.12. Let $\alpha \in K/F$, then α is algebraic over F if and only if $[F(\alpha) : F]$ is finite.

Corollary 4.1.13. A finite field extension is algebraic. Therefore, if $\alpha_1, \ldots, \alpha_n \in K$ are algebraic over F, then $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$, and $F(\alpha_1, \ldots, \alpha_n)/F$ is algebraic.

Theorem 4.1.14. Let K/F be a field extension, then the set $E \subseteq K$ of all algebraic elements over F is a subfield of K containing F.

Theorem 4.1.15. Let $L/K/F$ be a tower of field extension, then L/F is algebraic if and only if L/K and K/F are both algebraic.

Theorem 4.1.16. Let $f \in F[x]$ be a non-constant polynomial, then there exists a field extension K/F such that $[K : F] \leq \deg(f)$ and f has a root in K.

Corollary 4.1.17. Let $f \in F[x]$ be a non-constant polynomial, then there exists a field extension K/F such that $[K : F] \leq \deg(f)!$ and f is split over K.

Definition 4.1.18 (Splitting Field)**.** Let $f \in F[x]$ be a non-constant polynomial. A field extension K/F is called a splitting field of f over F if 1) f splits into linear factors $a \cdot (x - \alpha_1) \cdots (x - \alpha_n)$ over K for $a \in F$ and $\alpha_i \in K$ are roots of f in K, and 2) $K = F(\alpha_1, \ldots, \alpha_n)$.

Corollary 4.1.19. A non-constant polynomial $f \in F[x]$ has a splitting field of degree at most $\deg(f)!$.

Remark 4.1.20. Let K/F be a field extension such that $f(x) \in F[x]$ splits over K, then K contains a unique splitting field of F.

Definition 4.1.21 (Extension)**.** Suppose K/F and K'/F' are field extensions, and $\varphi : F \to F'$ is a field homomorphism, then an extension ψ of φ is a field homomorphism $\psi : K \to K'$ where with $\psi(a) = \varphi(a)$ for all $a \in F$.

Remark 4.1.22. If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, then $\varphi(f) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0) \in F'[x]$.

Proposition 4.1.23. Suppose $F(\alpha)/F$ is a finite field extension, and let $f = m_\alpha \in F[x]$, and suppose $\varphi : F \to F'$ is a field homomorphism, and K'/F' is another field extension, then

- if $\psi : K \to K'$ is an extension of φ, then $\psi(\alpha)$ is a root of the polynomial $\varphi(f) \in F'[x]$,
- for any root α' of $\varphi(f)$ in K', there exists a unique extension $\psi : K \to K'$ of φ such that the image $\psi(\alpha) = \alpha'$.

Corollary 4.1.24. With the setting above, the number of extensions of φ is at most $\deg(f) = \deg(\alpha) = [K : F]$.

Theorem 4.1.25. Let K/F be the splitting field of a non-constant polynomial $f(x) \in F[x]$ and $\varphi : F \to F'$ is a field isomorphism. Let K'/F' be a splitting field of $\varphi(f) \in F'[x]$, then there exists a field isomorphism $\psi : K \to K'$ that extends φ.

Corollary 4.1.26. Let $f \in F[x]$ be a non-constant polynomial and K/F and K'/F are both splitting field of the polynomial, then K/F and K'/F are isomorphic over F.

4.2 Finite Fields

Definition 4.2.1 (Characteristic)**.** The characteristic of a field F is the smallest positive integer n such that the n-term summation $\sum_n 1_F = 0_F$. Suppose such n exists in F, then we say the field has characteristic p; if not, we say the field has characteristic 0.

Proposition 4.2.2. A field F either has characteristic 0 or characteristic $p > 0$ for a prime integer p. Indeed, this is generated by the kernel of the unique morphism $\mathbb{Z} \to F$ since $\mathbb{Z}$ is initial in the category of fields.

Proposition 4.2.3 (Freshman's Dream)**.** Let F be a field with characteristic $p > 0$, then $(a+b)^p = a^p + b^p$ for all $a, b \in F$.

Corollary 4.2.4. Let F be a field with characteristic $p > 0$, then $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ for any integer k.

Definition 4.2.5 (Frobenius Homomorphism)**.** Let F be a field of characteristic $p > 0$, then there is a field homomorphism

$$\begin{aligned} f : F &\to F \\ x &\mapsto x^p \end{aligned}$$

.

Definition 4.2.6 (Multiplicity, Simply Root, Derivative)**.** Let $f(x) \in F[x]$ be a polynomial over a field F of positive charactersitic. Suppose $\alpha \in F$ is a root of f, then $f(\alpha) = 0$, so $f(x) = (x-\alpha)^k \cdot h(x)$ for some $h(x) \in F[x]$ and some positive integer k such that $h(\alpha) \neq 0$. This number k is called the multiplicity of α.

If $k = 1$, then α is called a simple root of f.

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, then the derivative of $f(x)$ is defined by $f'(x) = n a_n x^n + \cdots + x + a_1$.

Lemma 4.2.7. Let $f(x) \in F[x]$ be a polynomial and $\alpha \in F$ be a root of f, then α is a simple root if and only if $f'(\alpha) \neq 0$.

Corollary 4.2.8. If $\gcd(f, f') = 1$, then every root of f is simple.

Remark 4.2.9. If $\gcd(f, f') = 1$ over F, and let K/F be a field extension, then since $\gcd(f, f') = 1$ over K as well, then all roots of f over K are simple over a splitting field.

Definition 4.2.10 (Finite Field)**.** We say F is a finite field if it has finitely many elements.

Remark 4.2.11. The characteristic of a finite field is positive. Therefore, there is a prime subfield $\mathbb{Z}/p\mathbb{Z} \subseteq F$. Therefore, if we denote $[F : \mathbb{Z}/p\mathbb{Z}] = n$, then $x_1, \ldots, x_n$ form a basis of $F/\mathbb{Z}/p\mathbb{Z}$, so F is the set of $\mathbb{Z}/p\mathbb{Z}$-linear combinations, so F has order p^n for some positive integer n.

Theorem 4.2.12. Let p be any prime integer and $n > 0$ be any integer, then there exists a unique field with p^n elements, up to isomorphism.

Example 4.2.13. $\mathbb{F}_{p^2} \cong \mathbb{Z}/p^2\mathbb{Z}$.

Theorem 4.2.14 (May 2022, Problem 4)**.** Let F be a field and $A \subseteq F^\times$ be a finite multiplicative subgroup, then A is cyclic.

Corollary 4.2.15. $\mathbb{F}_q^\times$ is cyclic for $q = p^n$. In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Definition 4.2.16 (Simple)**.** A field extension K/F is simple if there exists some $\alpha \in K$ such that $K = F(\alpha)$.

Corollary 4.2.17. Every finite extension of a finite field is simple.

Remark 4.2.18. Let $q = p^n$ and $s = p^m$, then $\mathbb{F}_q/F_s$ is a field extension if and only if $m \mid n$.

Theorem 4.2.19 (Gauss)**.** Consider the ring $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n, then the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1, 2, 4, p^k$, or $2p^k$ for some positive integer k and some prime integer $p > 0$.

Exercise 4.2.20 (May 2022, Problem 4)**.** (a) Let $k = \mathbb{Z}/p\mathbb{Z}$ be the finite field of order p, where p is a prime. Let K/k be a finite field extension of degree m. Prove that the elements of K are the roots of the polynomial $x^{p^m} - x$ over k.

(b) Prove that every irreducible polynomial $f(x) \in k[x]$ is separable.

Exercise 4.2.21 (August 2020, Problem 4)**.** Let $\mathbb{F}$ be a field of characteristic $p > 0$ and $p \neq 3$. If α is a root of the polynomial $f(x) = x^p - x + 3$, in an extension of the field $\mathbb{F}$, show that $f(x)$ has p distinct roots in the field $\mathbb{F}(\alpha)$.

Exercise 4.2.22 (August 2019, Problem 5)**.** Let $p > 2$ be a prime integer.

(a) Show that for any integer n, $n^p \equiv n \pmod{p}$.

(b) Let k be a field of characteristic p and let $f(x) = x^p - x - a \in k[x]$, $a \in k$. Show that

(i) if $f(x)$ has a root in k, then $f(x)$ has all its roots in k;

(ii) if $f(x)$ does not have any root in k, then $f(x)$ is irreducible in $k[x]$;

(iii) in case (ii) above, the Galois group of $f(x)$ is cyclic of order p.

4.3 Normal and Separable Extensions

Lemma 4.3.1. Let E/F be a finite field extension and $\sigma : F \to L$ is a field homomorphism, then there exists a finite field extension M/L and an extension $\tau : E \to M$ over σ.

Proposition 4.3.2. Let E/F be a finite field extension, then the following are equivalent:

- E is the splitting field of some polynomial f over F;
- for every finite extension M/E and every field homomorphism $\sigma : E \to M$ over F, we have $\sigma(E) = E$, i.e., σ fixes the base field;
- every irreducible polynomial $f(x) \in F[x]$ that has a root in E splits over E.

Definition 4.3.3 (Normal Extension)**.** We say E/F is a normal extension if any of the above holds.

Remark 4.3.4. If $E = F(\alpha_1, \ldots, \alpha_n)$, then E/F is normal if and only if m_{α_i} splits over E for all i.

Corollary 4.3.5. If $L/E/F$ is a tower of field extensions and L/F is normal, then so is L/E.

Remark 4.3.6. Note that E/F may not be normal; also, if L/E and E/F are both normal, L/F may not be normal.

Lemma 4.3.7. Let $f(x) \in F[x]$ be a non-constant polynomial, then the following are equivalent:

- $\gcd(f, f') = 1$;
- over any field extension K/F, f has no multiple roots;
- there exists a field extension K/F such that f is split over K and has no multiple roots.

Definition 4.3.8 (Separable polynomial)**.** A non-constant polynomial $f(x) \in F[x]$ is separable if f satisfies any of the above.

Corollary 4.3.9.
- If $f(x) \in F[x]$ is separable over F, then for any field extension K/F, $f(x) \in K[x]$ is also separable over K.
- If f is separable and $g \mid f$ is a non-constant divisor, then g is separable as well.

Corollary 4.3.10. Let $F(\alpha)/F$ be an algebraic field extension, where $f(\alpha) = 0$ for a separable polynomial $f(x) \in F[x]$, then the minimal polynomial $m_\alpha(x)$ is separable.

Proposition 4.3.11. An irreducible polynomial $f(x) \in F[x]$ is separable if and only if $f'(x) \neq 0$.

Definition 4.3.12 (Perfect)**.** A field F is perfect if either it has characteristic 0, or it has characteristic $p > 0$ and $F^\times = (F^\times)^p$.

Remark 4.3.13. Let F be a field of characteristic $p > 0$ and let $a \in F^\times$, then $f(x) = x^p - a$ is not separable. In fact, $f(x)$ is irreducible if and only if $a \notin (F^\times)^p$.

Proposition 4.3.14. Every irreducible polynomial over a perfect field is separable.

Example 4.3.15. Finite fields are perfect.

Definition 4.3.16 (Separable)**.** Let K/F be a field extension, and $\alpha \in K$ be an algebraic element over F, then α is separable over F if the minimal polynomial m_α is separable.

Remark 4.3.17. If F is perfect, then every algebraic element α is separable.

Lemma 4.3.18. Let $L/K/F$ be a tower, and $\alpha \in L$ is separable over F, then α is separable over K.

Lemma 4.3.19. Let K/F be a finite field extension and $\sigma : K \to L$ be a field homomorphism, then there are at most $[K : F]$ extensions $K \to L$ of σ.

Definition 4.3.20 (Separable Extension)**.** A finite field extension $F(\alpha)/F$ is separable if there exists a field homomorphism $\sigma : F \to L$ that has exactly $[K : F]$ extensions $K \to L$.

Proposition 4.3.21. A finite field extension $F(\alpha)/F$ is separable if and only if α is separable over F.

Lemma 4.3.22. let F be an infinite field and L/F be a field extension, and let $g(x_1, \ldots, x_n) \in L[x_1, \ldots, x_n]$ be a non-zero polynomial, then there exists $a_1, \ldots, a_n \in F$ such that $g(a_1, \ldots, a_n) \neq 0$.

Corollary 4.3.23. Let $g_1, \ldots, g_m \in L[x_1, \ldots, x_n]$ be distinct polynomials, then there exists $a_1, \ldots, a_n \in F$ such that $g_i(a_1, \ldots, a_n)$ are distinct for all i.

Theorem 4.3.24 (Primitive Element Theorem)**.** Let K/F be a finite separable extension, then $K = F(\alpha)$ for some $\alpha \in K$.

Proposition 4.3.25. Let $L/K/F$ be finite field extensions, then L/F is separable if and only if L/K and K/F are separable.

Corollary 4.3.26. Let K/F be a finite field extension, then the following are equivalent:
- K/F is separable;
- every $\alpha \in K$ is separable over F;
- $K = F(\alpha_1, \ldots, \alpha_n)$ for separable elements $\alpha_i \in F$;
- $K = F(\alpha)$ for some separable element $\alpha \in F$.

Corollary 4.3.27. A finite field extension over a perfect field is separable.

4.4 Galois Theory

Definition 4.4.1 (Galois Group)**.** The Galois group $\mathrm{Gal}(E/F)$ is the set of field E-automorphism over F. In particular, each automorphism fixes F and is F-linear.

Proposition 4.4.2. Suppose E/F is a finite field extension, then $|\mathrm{Gal}(E/F)| \leq [E:F]$, with equality holds if and only if E/F is normal and separable.

Definition 4.4.3 (Galois Extension)**.** A finite field extension E/F is Galois if $|\mathrm{Gal}(E/F)| = [E:F]$, i.e., E/F is normal and separable.

Remark 4.4.4. Let E/F be Galois and G be the Galois group, then $E = F(\alpha)$ for some $\alpha \in E$. Take $f = m_\alpha$, then f splits over E and has exactly $[E:F]$ in E. Let X be the set of roots of f in E, then any automorphism in the Galois group sends a root to another root. This induces an action of G on X, and this action is simple and transitive.

Theorem 4.4.5 (Artin)**.** Let E be any field and G be a finite subgroup of $\mathrm{Aut}(E)$, then set $F = E^G = \{x \in E : \sigma(x) = x \, \forall \sigma \in G\}$ to be the fixed field of E over G, then E/F is a field extension. Moreover, this is Galois with $\mathrm{Gal}(E/F) = G$.

Example 4.4.6. Let K be a field, then $K(x_1, \ldots, x_n)$ is the field of fractions of $K[x_1, \ldots, x_n]$ given by S_n.

Example 4.4.7. Let $G \hookrightarrow S_n \subseteq \mathrm{Aut}(E)$, then $\mathrm{Gal}(E/E^G) = G$, so every finite group is the Galois group of some field extension.

Definition 4.4.8 (Compositum)**.** Let M/F be a field extension, and let K and L be intermediate extensions of this extension, then KL is the smallest subfield of M containing both K and L, called the compositum of K and L in M over F.

Theorem 4.4.9 (Fundamental Theorem of Galois Theory)**.** Let E/F be a Galois extension and $G = \mathrm{Gal}(E/F)$.

- Let L be an intermediate field extension $E/L/F$, then there is a subgroup of G given by $\{\sigma \in G \mid \sigma(x) = x \, \forall x \in L\} = \mathrm{Gal}(E/L)$, i.e., the Galois group of E over L is the E-automorphisms over L.

  Conversely, let $H \subseteq G$ be a subgroup, then there exists a subfield $L = E^H$ with $E/L/F$ that fixes H over E.

  This is a bijective correspondence (and inverses and inclusion-reversing) given by $L \mapsto \mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/F) = G$, and $H \mapsto E^H$, respectively.

  Moreover, if $E/L_2/L_1/F$ is a tower, then $\mathrm{Gal}(E/L_1) \supseteq \mathrm{Gal}(E/L_2)$; similarly, if $H_1 \subseteq H_2 \subseteq G$, then $E^{H_1} \supseteq E^{H_2}$.

  Moreover, normal subgroups H of G corresponds to normal bottom extensions L/F.

  More formally, this gives a correspondence that sends subfields L of E containing F to subgroups H of G by elements of G fixing L, and sends subgroups of H of G back to subfields L of E containing F by elements of E fixed by H. Therefore, this is an association between subgroups of Galois groups and their fixed fields.

- Subgroup indices correspond to extension degrees, so $[E:L] = |H|$ and $[L:F] = |G:H|$.

- Let $\sigma \in G$ and $H \subseteq G$, then the conjugation $\sigma H \sigma^{-1} \subseteq G$, and $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$.

- The lattice of subgroups of G is the same as the lattice of intermediate fields of E/F turned upside down, with degree of extensions over F are the same as the index of subgroups of G.

- The upper tower E/L is always Galois with Galois group H.

- The lower tower L/F is Galois if and only if L/F is normal, if and only if H is a normal subgroup of G. If this is the case, then $\mathrm{Gal}(E/F) \cong G/H$.

  Alternatively, if H is a subgroup of G, then E^H/F is normal if and only if $H \lhd G$. If this is the case, then $\mathrm{Gal}(E^H/F) \cong G/H$.

- Intersections of subgroups $H \cap K$ correspond to field compositums $E^H E^K$; joins of subgroups HK corresponds to field intersections $E \cap K$.

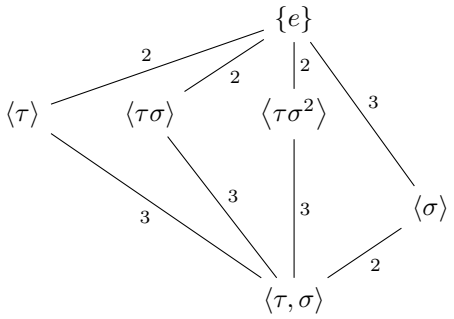
  More formally, suppose L_1, L_2 are intermediate field extensions of E/F, and suppose L_1/F is Galois, then L_1L_2/L_2 is Galois. Therefore, we have an isomorphism

  $$\mathrm{Gal}(L_1L_2/L_2) \cong \mathrm{Gal}(L_1/L_1 \cap L_2).$$

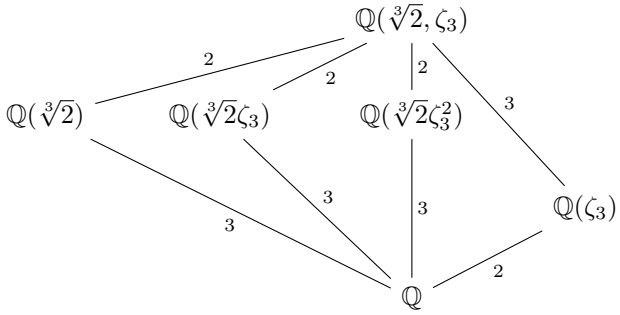
  In particular, if $L_1 \cap L_2 = F$, i.e., they are linearly disjoint over F, then $\mathrm{Gal}(L_1/L_2/L_2) \cong \mathrm{Gal}(L_1/F)$.

Theorem 4.4.10. With the notations above, if L_1/F and L_2/F are both Galois, then L_1L_2/F is Galois. Moreover, if $L_1 \cap L_2 = F$, then $\mathrm{Gal}(L_1L_2/F) \cong \mathrm{Gal}(L_1/F) \times \mathrm{Gal}(L_2/F)$ is an internal direct product.

Example 4.4.11. Consider $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$, which is the splitting field of $x^3 - 2$. The Galois group is the dihedral group D_3 of order 6. Let σ be such that $\sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$ and $\zeta_3 \mapsto \zeta_3$, and let τ be such that $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ and $\zeta_3 \mapsto \zeta_3^2$, then $D_3 \cong \langle \sigma, \tau \rangle$. The Galois correspondence gives a correspondence between



and



Exercise 4.4.12 (August 2021, Problem 4)**.** Let F be a field, $F[x]$ be the ring of polynomials over F, and $F(x)$ be the field of fractions of (the integral domain) $F[x]$. The map $F \to F(x)$ is an injective field homomorphism, so we view F as a subfield of $F(x)$: in this way, $F \subseteq F(x)$. In what follows, provide justification.

(a) Prove that the function $\sigma : F(x) \to F(x)$ given by

$$\sigma\left(\frac{f(x)}{g(x)}\right) := \frac{f(x+1)}{g(x+1)}$$

is a well-defined automorphism of the field $F(x)$. Prove that $\sigma \in \mathrm{Gal}(F(x)/F)$.

(b) Let G be the (cyclic) subgroup of $\mathrm{Gal}(F(x)/F)$ generated by σ. What is the order of G?

(c) Let $F := \mathbb{F}_2$, the field of order 2, an $E \subseteq \mathbb{F}_2(x)$ be the intermediate field corresponding to the subgroup $G \leq \mathrm{Gal}(\mathbb{F}_2(x)/\mathbb{F}_2)$ as in (b). Prove that $[E : \mathbb{F}_2] \geq 2$.

Exercise 4.4.13 (January 2021, Problem 4). (a) Let $f(x) = x^4 + 4x^3 + 6x^2 + 4x \in \mathbb{Q}[x]$ and E be a splitting field of $f(x)$. Does $f(x)$ have four pairwise distinct roots in E?

(b) For E as in part (a), what is the order of the Galois group, $|\mathrm{Gal}(E/\mathbb{Q})|$?

(c) For E as in part (a), is the extension $E/\mathbb{Q}$ a Galois extension?

Exercise 4.4.14 (August 2019, Problem 4). Consider the polynomial $f(x) = x^4 - 2$ on $\mathbb{Q}[x]$.

(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Let L denote the splitting field of $f(x)$ and let G denote its Galois group over $\mathbb{Q}$. Determine L and G. Also find a relation between the generators of G.

Exercise 4.4.15 (May 2019, Problem 5). Let K be the splitting field of $x^6 + 3$ over $\mathbb{Q}$.

(a) Compute the Galois group of K over $\mathbb{Q}$.

(b) How many subfields of K are there, which have degree 3 over $\mathbb{Q}$?

Exercise 4.4.16 (August 2018, Problem 4). Let L be a Galois extension of $\mathbb{Q}$ of order 100. Show that there exists a chain of extensions $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq K_4 = L$ where each K_{i+1} is a Galois extension of K_i.

Exercise 4.4.17 (August 2018, Problem 5). Show that the polynomial $x^6 - 3 \in \mathbb{Q}[x]$ is irreducible and determine its Galois group.

Exercise 4.4.18 (May 2018, Problem 5). (a) Find the Galois group of the polynomial $p(x) = x^3 - 10$ over the field $K = \mathbb{Q}(\sqrt{2})$.

(b) Let $q(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p \geq 2$. Show that if $q(x)$ has exactly two non-real roots (i.e., two complex roots) then the Galois group of $q(x)$ is isomorphic to S_p.

4.5 Cyclotomic Extensions

Definition 4.5.1 (Cyclotomic Extension). Let F be a field, and let n be an integer that is relatively prime to $\mathrm{char}(F)$ for positive characteristic, and is any integer for zero characteristic. The polynomial $f(x) = x^n - 1$ is separable over F, and the splitting field of $f(x)$ over F is a Galois field extension F_n/F, called the n-cyclotomic field extension of F.

Remark 4.5.2. The field F_n/F is generated by a primitive root, so $F_n = F(\zeta_n)$. Take any $\sigma \in \mathrm{Gal}(F_n/F)$ with $\sigma(\zeta_n) = (\zeta_n)^k$ for some integer k such that $\gcd(k, n) = 1$, then the map

$$\begin{aligned} \chi : \mathrm{Gal}(F_n/F) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto [k]_n \end{aligned}$$

is an injective group homomorphism. Therefore, we identify $\mathrm{Gal}(F_n/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ as a subgroup, so the Galois group must be abelian.

Remark 4.5.3. Let $F = \mathbb{Q}$, and let Φ_n be the minimal polynomial of ζ_n of degree n, then $\Phi_n \in \mathbb{Z}[x]$ by Gauss Lemma since it divides $x^n - 1$ in $\mathbb{Z}[x]$. Such Φ_n is called the nth cyclotomic polynomial over $\mathbb{Q}$.

Lemma 4.5.4. Let p be a prime integer such that $p \nmid n$, then $(\zeta_n)^p$ is a root of Φ_n.

Corollary 4.5.5. All primitive roots of unity of degree n are the roots of Φ_n, and in particular $\deg(\Phi_n) \geq \varphi(n)$.

Theorem 4.5.6. $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore, $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$, and $\Phi_n(x)$ is the product of linear factors $(x - \zeta)$ where ζ is a primitive nth root of unity.

Corollary 4.5.7.

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$. In particular, $\Phi_n(x)$ divides $x^n - 1$.
- $\Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + 1$ for prime p.
- $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$.
- If n is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$. More generally, we have the following: if p is prime and $p \nmid n$, then $\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$; if p is prime and $p \mid n$, then $\Phi_{np}(x) = \Phi_n(x^p)$.

Remark 4.5.8. All cyclotomic polynomials are irreducible polynomials over $\mathbb{Q}$.

Exercise 4.5.9 (August 2020, Problem 5)**.** (a) Compute a factorization for $x^{26} - 1$ into irreducible polynomials over $\mathbb{Z}$.

(b) Find the number of all subfields of the splitting field K of $x^{26} - 1$ over $\mathbb{Q}$ and prove that all of them are Galois over $\mathbb{Q}$.

Exercise 4.5.10 (January 2019, Problem 4)**.** (a) Find the cyclotomic polynomial $\Phi_{20}(x)$ for 20th roots of unity over any field K whose characteristic is relatively prime to 20.

(b) Let $F = \mathbb{Z}/p\mathbb{Z}$, p a prime, and let K be an extension of F such that $[K : F] = n$. Prove that the elements of K are the roots of $x^{p^n} - x = 0$.

(c) Show that every irreducible factor of $\Phi_k(x)$, $k = p^n - 1$, in $F[x]$ has degree n.

4.6 Galois Group of Polynomials

Definition 4.6.1. Let $f(x) \in F[x]$ be a separable polynomial over a field F of characteristic 0. Take E/F as the splitting field of $f(x)$, so this is an Galois extension. $\mathrm{Gal}(E/F)$ is the Galois group of $f(x) \in F[x]$.

Proposition 4.6.2. Let E/F be Galois and $\alpha \in F$. Let S be the set of distinct elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(E/F)$, then $\deg(\alpha) = |S|$ and $m_\alpha = \prod_{\beta \in S} (x - \beta)$.

Example 4.6.3. $\mathrm{Gal}(x^n - 1) = (\mathbb{Z}/n\mathbb{Z})^\times$ over $\mathbb{Q}$.

We will now focus on using resolvent, discriminant, and other techniques to find Galois groups of polynomials, especially for cubic and quartic ones. Recall that:

- Let $f(x)$ be a polynomial of degree n and with Galois group G, then there exists an embedding $G \hookrightarrow S_n$. Therefore, G is a subgroup of S_n.
- Suppose $f(x)$ is a separable polynomial of degree n with Galois group G, then f is irreducible if and only if G acts transitively on the roots, i.e., G is a transitive subgroup of S_n, that is, for every $i, j \in \{1, \ldots, n\}$, there exists $\sigma \in G$ such that $\sigma(i) = j$.

- By a change of variables, any cubic polynomial has the form $x^3 + ax + b$, and any quartic polynomial has the form $x^4 + qx^2 + rx + s$.

Remark 4.6.4.
- The transitive subgroups of S_3 are S_3 and A_3.
- The transitive subgroups of S_4 are the cyclic group C_4, the Klein-4 group V_4, the dihedral group D_4, the alternating group A_4, as well as the symmetric group S_4. Note that here V_4 is of the form $\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. The other form of V_4, $\{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$ is not transitive.

Proposition 4.6.5. Suppose $G \subseteq S_n$ is a transitive subgroup, and suppose G contains an $(n-1)$-cycle and a transposition, then $G = S_n$.

Corollary 4.6.6. S_n is generated by a n-cycle and a transposition if and only if n is prime.

Proposition 4.6.7. If a polynomial $f(x) \in \mathbb{Z}[x]$ has exactly two non-real roots, then the complex conjugation, as a transposition, is an element of the Galois group.

Definition 4.6.8 (Discriminant)**.** The discriminant of a monic polynomial $f(x) \in \mathbb{Z}[x]$ is $\Delta = \prod_{1 \le i < j \le n} (r_i - r_j)^2$ where r_i's are roots of $f(x)$.

Remark 4.6.9. The discriminant of $x^3 + ax + b$ is $-4a^3 - 27b^2$.

Proposition 4.6.10. If the discriminant is a square, then the Galois group $G \subseteq S_n$ must be a subgroup of A_n. Indeed, this means the product of differences of roots is in $\mathbb{Q}$, which is fixed at most by A_n.

Definition 4.6.11 (Resolvent)**.** Let $f(x)$ be a polynomial with roots $x_1, \ldots, x_n$, then the resolvent is the polynomial whose roots as the product of pairwise sum of roots of the polynomial.

Remark 4.6.12. In particular, given a quartic polynomial $f(x) = x^4 + qx^2 + rx + s$, it has a resolvent cubic $g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2$, given by $\alpha = (x_1 + x_2)(x_3 + x_4)$, $\beta = (x_1 + x_3)(x_2 + x_4)$, $\gamma = (x_1 + x_4)(x_2 + x_3)$ where x_i's are roots of $f(x)$, so that $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$.

Remark 4.6.13. To find the Galois group of a quartic polynomial, we have the following algorithm:

- Note that the Galois group G must embeds into S_4, so it is always a subgroup of S_4.
- If the determinant Δ is a perfect square, then G embeds in A_4.
- If the resolvent $g(x)$ is irreducible, then G is S_4 or A_4 depending on the test above.
- If the resolvent $g(x)$ is not irreducible, then G is a subgroup of D_4. Now if the polynomial splits, then this is V_4; if the polynomial does not split, then this is either D_4 or $\mathbb{Z}/4\mathbb{Z}$. If $f(x)$ is irreducible over $F(\sqrt{\Delta})$, then it is D_4, otherwise it is $\mathbb{Z}/4\mathbb{Z}$.

Exercise 4.6.14 (January 2020, Problem 5)**.**
(a) Describe the subgroups of S_4 that can occur as Galois group of an irreducible quartic polynomial.

(b) Determine the Galois group of the irreducible polynomial $x^4 + 2x^2 + 4$. (You can use the fact that a quartic polynomial $f(x) = x^4 + qx^2 + rx + s$ has resolvent cubic $g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2$.)

Exercise 4.6.15 (January 2019, Problem 5)**.** Consider $f(x) = x^5 - 4x - 2 \in \mathbb{Q}[x]$.

(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Let K be the splitting field of $f(x)$ in $\bar{\mathbb{Q}}$. Find the Galois group $G(K/\mathbb{Q})$ of $f(x)$ over $\mathbb{Q}$.