Problems and Solutions in Abstract Algebra

Kaizhao Liu

August 2022

Contents

1 Groups

1.1 General Constructions

1.1.1 Direct Products

Theorem 1.1. *Let G be a group with normal subgroups H and K. If $HK = G$ and $H \cap K = 1$, then $G \simeq H \times K$.*

Example 1.1. *Let H be a subgroup of finite index n of a group G. Then $g \in Z(G) \Longrightarrow g^n \in H$.*

1.2 Concrete Groups

Example 1.2 (Fundamental Theorem of Finite Abelian Group)**.**
Primary decomposition: every finite abelian group is a direct sum of primary cyclic group.

Example 1.3 (Group of prime order)**.** *If p is a prime and $|G| = p$, then G is a cyclic group.*

Example 1.4. *If p is a prime and $|G| = p^2$, then G is abelian. Therefore, G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

For example we have

Example 1.5 (Group of order 4)**.** *Every group of order* 4 *is isomorphic to either* $\mathbb{Z}_4$ *or the* 4*-group* $\mathbf{V}$.

Example 1.6. *If* $m \geq 3$*, then* $U(\mathbb{Z}_{2^m}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$

Proof. $|U(\mathbb{Z}_{2^m})| = 2^{m-1}$. So it is a 2-group.
$5^{2^{m-3}} = (1+4)^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m$ by induction and the binomial theorem. So 5 has order 2^s for some $s \geq m-2$.
Of course -1 has order 2. We claim that $\langle -1 \rangle \cap \langle 5 \rangle = 1$. □

Example 1.7. *If* p *is an odd prime, the multilpicative group* $U(\mathbb{Z}_{p^n}) \cong \mathbb{Z}_{(p-1)p^{n-1}}$.

1.2.1 Cyclic Groups

Theorem 1.2 (Euler φ-function)**.** *The Euler* φ*-function is defined as follows:*

$$\varphi(1) = 1; \quad \varphi(n) = |\{k : 1 \leq k < n, (k,n) = 1\}| \, (n > 1)$$

(i) If G *is cyclic of order* n*, then the number of generators of* G *is* $\varphi(n)$.
(ii) If $(r,s) = 1$*, then* $\varphi(rs) = \varphi(r)\varphi(s)$.
(iii) If p *is prime, then* $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.
(iv) If the distinct prime divisor of n *are* $p_1, \cdots, p_t$*, then* $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_t})$.
(v) If $(r,s) = 1$*, then* $s^{\varphi(r)} \equiv 1 \mod r$.

Proof. Suppose G is a cyclic group.
(i) If $G = \langle a \rangle$ and $|G| = n$, then a^k is also a generator of G if and only if $(k,n) = 1$.
(ii) □

Theorem 1.3. *If* G *is a cyclic group of order* n*, then there exists a unique subgroup of order* d *for every divisor* d *of* n.

Proof. If $G = \langle a \rangle$, then $\left\langle a^{\frac{n}{d}} \right\rangle$ is a subgroup of order d.

Assume $S = \langle b \rangle$ is a subgroup of order d, then $b^d = 1$ and $b = a^m$ for some m. So $md = kn$ for some integer k, and $b = (a^{\frac{n}{d}})^k$. Therefore $\langle b \rangle \leq \left\langle a^{\frac{n}{d}} \right\rangle$, and the inclusion is equality because both subgroups have order n. □

Example 1.8. *If* n *is a positive integer, then* $n = \sum_{d|n} \varphi(d)$.

Proof. This identity can be easily proved by listing all fractions with denominator n and reducing these fractions to simplified fractions.

Here we prove this identity in a group-theoritic manner. Consider a cyclic group G of order n. If C is a cyclic subgroup of a group G, let $\text{gen}(C)$ denote the set of all its generators. Every element in G generates a cyclic subgroup. If we put the elements which generate the same cyclic subgroup together, we get a disjoint union decomposition of G: $G = \bigcup \text{gen}(C)$. But every cyclic subgroup of G is of order d for some $d|n$. Therefore, $n = |G| = \sum_{d|n} |\text{gen}(C_d)| = \sum_{d|n} \varphi(d)$. □

Example 1.9. *If* F *is a field and* G *is a finite subgroup of* $F^\times$*, then* G *is cyclic.*

Proof. If $a \in G$ satisfies $a^d = 1$, then a is a root of the polynomial $x^d - 1 \in F[x]$ in F. Since a polynomial of degree d over a field has at most d roots, □

1.2.2 Symmetric Groups

Lemma 1.1. *If* $\alpha, \beta \in S_n$*, then* $\alpha\beta\alpha^{-1}$ *is the permutation with the same cyclic structure as* β *which is obtained by applying* α *to the symbols in* β.

Theorem 1.4. *Permutations* $\alpha, \beta \in S_n$ *are conjugate if and only if they have the same cycle structure.*

Proof. The lemma above shows that conjugate permutations do have the same cycle structure.

For the converse, define $\gamma \in S_n$ as follows: place the complete factorization of α over that of β so that the cycles of the same length correspond, and let γ be the function sending the top to the bottom. γ is a permutation for every i between 1 and n occurs exactly once in a complete factorization, and $\gamma\alpha\gamma^{-1} = \beta$. □

Corollary 1.4.1. *A subgroup H of S_n is a normal subgroup if and only if whenever $a \in H$, then every β having the same cycle structure as α also lies in H.*

Theorem 1.5 (Simplicity of A_n)**.** *A_n is simple for all $n \geq 5$.*

Proof. The proof consists of several steps. All of them focus on 3-cycles.

First, we are going to prove that A_5 is simple.

Second, let $H \lhd A_n$, where $n \geq 5$. If H contains a 3-cycle, then $H = A_n$.

Third, we are going to prove that A_6 is simple.

Finally, let $n > 6$. Let $H \neq 1$ be a normal subgroup of A_n. If $\beta \in H$ and $\beta \neq 1$, then there is an i with $\beta(i) = j \neq i$. If α is a 3-cycle fixing i and moving j, then α and β do not commute: $\beta\alpha(i) = \beta(i) = j$ and $\alpha\beta(i) = \alpha(j) \neq j$. Therefore, their commutator is not the identity. $(\alpha\beta\alpha^{-1})\beta^{-1}$ lies in the normal subgroup H. $\alpha(\beta\alpha\beta^{-1})$ is a product of two 3-cycles, thus it moves at most 6 symbols. If $F = \{\gamma \in A_m : \gamma \text{ fixed the other symbols}\}$, then $F \simeq A_6$ and $\alpha\beta\alpha^{-1}\beta^{-1} \in H \cap F \lhd F$. Since A_6 is simple, $H \cap F = F$ so $F \leq H$. Therefore H contains a 3-cycle, $H = A_n$. □

1.3 Group Actions

Definition 1.1 (group actions)**.** A (left) group action of G on a set X is a map

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

that satisfies the following conditions:
(1) $g(g'x) = (gg')x$ for all $x \in X$ and all $g, g' \in G$.
(2) $1x = x$ for all $x \in X$, where 1 is the identity element of G.

Remark. *Equivalently, a group action of G on X can be defined as a group homomorphism τ from G to the symmetric group S_X of X.*

Two most important concept about group actions are **orbits** and **stabilizer**.

Lemma 1.2 (Burnside's lemma)**.** *Let G be a finite group and let X be a finite G-set. For every $g \in G$, let $X^g \subset G$ be the set of elements x of X which are fixed under the action of g, and let $\chi_X(g) = |X^g|$. Then:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \chi_X(g)$$

In other words, the number of orbits is the average of the number of fixed points of the elements of the group.

Proof. Define $f(g, x) = 1_{gx=x}$. Let us compute in two different ways the sum $S = \sum_{(g,x) \in G \times X} f(g, x)$. □

Definition 1.2 (k-transitivity)**.** Let X be a G-set of degree n and let $k \leq n$ be a positive integer. Then X is k-transitive if, for every pair of k-tuples having distinct entries in X, say, $(x_1, \cdots, x_k)$ and $(y_1, \cdots, y_k)$, there is $g \in G$ with $gx_i = y_i$ for $i = 1, \cdots, k$.

1.3.1 Sylow Theorems

Theorem 1.6 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

J.H.McKay. First recall how we dealt with the rather simple case $p = 2$. We pair a and a^{-1} for all $a \in G$ and count their numbers. The J.H.McKay's proof is actually a generalization of this idea.

Define

$$X = \{(a_1, \cdots, a_p) \in G \times \cdots \times G : a_1 a_2 \cdots a_p = 1\}$$

Then $|X| = |G|^{p-1}$. View X as a Z_p-set by defining the action to be cyclically permuting the coordinates. Verify that it is well-defined.

Each orbit of X has either 1 or p elements for $|Z_p| = p$. If one orbit has only one element, then the element is a p-tuple having all its coordinates equal, say $a_i = a\ \forall i$. Thus $a^p = 1$. $(1, \cdots, 1)$ is such an orbit. Were this the only orbit, then we would have $|X| = 1 + kp$ for some integer $k \geq 0$, that is, $|G|^{p-1} \equiv 1 \mod p$, which is a contradiction. □

Proof. Here is a proof by induction. First we prove this result for finite abelian groups, then we use the class equation to reduce the general case.

For abelian group G, suppose $|G| = pm$, where $m \geq 1$. When $m = 1$, the statement is obvious. For the inductive step, choose $x \in G$ of order $t > 1$. If $p|t$, then $x^{\frac{t}{p}}$ has order p. If $p \nmid t$, since G is abelian, $\langle x \rangle$ is a normal subgroup of G, and $G/\langle x \rangle$ is an abelian group of order $\frac{pm}{t}$. By induction, $G/\langle x \rangle$ contains an element y^* of order p. □

Theorem 1.7 (p-group)**.** *If p is a prime, then a p-group is a group in which every element has order a power of p.*

(i) A finite group G is a p-group if and only if $|G|$ is a power of p.

Now assume that G is a finite p-group.

(ii) $Z(G) \neq 1$.

(iii) If H is a proper subgroup of G, then $H < N_G(H)$.

(iv) Every maximal subgroup of G is normal and has index p.

(v) Let r_s be the number of subgroups of G having order p^s, then $r_s \equiv 1 \mod p$.

Proof. (i) If G is a p-group, assume that there is a prime $q \neq p$ which divides $|G|$. By Cauchy's theorem, G contains an element of order q, and this is a contradiction. Conversely, if $|G| = p^m$, then Lagrange's theorem shows that G is a p-group.

(ii) Consider the class equation $|G| = |Z(G)| + \sum [G : C_G(x_i)]$. Each $C_G(x_i)$ is a proper subgroup of G, and $[G : C_G(x_i)]$ is a power of p. Thus p divides $|Z(G)|$. □

Example 1.10. *If p is a prime, then every group G of order p^2 is abelian.*

Proof. If p-group G is not abelian, then $|Z(G)| = p$. Then $|G/Z(G)| = p$ is cyclic, which is a contradiction. □

Example 1.11. *Let K be a finite field of characteristic p with $q = p^f$ elements. Let $G = GL_n(K)$. The order of G is the number of K-bases of K^n. Hence $|G| = (q^n - 1)(q^n - 1) \cdots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - 1) = p^{f\frac{n(n-1)}{2}} m$, where $m = \prod_{i=1}^n (q^i - 1)$ is prime to p.*

Let S be the group of upper triangular matrices with diagonal entries equal to 1. It is a subgroup of G of order $q^{\frac{n(n-1)}{2}}$, hence it is a p-Sylow subgroup of G.

Theorem 1.8. *Let H be a subgroup of G and let S be a p-Sylow subgroup of G. There exists $g \in G$ s.t. $H \cap gSg^{-1}$ is a p-Sylow subgroup of H.*

Proof. The key is to consider H acting on $X = G/S$ by left multiplication. Notice that the stabliziers of the points of X are of the form $H \cap gSg^{-1}$, with $g \in G$. This is exactly the form of the group we are looking for.

Then we make use of the fact that S is a p-Sylow subgroup to conclude that $p \nmid |X|$. Hence there is at least one orbit $\mathcal{O} = Hx$ whose order is prime to p. The stablizier of x is the p-Sylow subfroup of H we sought. □

Corollary 1.8.1. *Here is a second proof of the first Sylow theorem.*

Proof. Let n be the order of G. We embed G into the symmetric group S_n by making G act on itself by left translations. We embed S_n in $GL_n(F_p)$ as follows: if $\sigma \in S_n$ and $(e_i)_{1 \leq i \leq n}$ is a basis of F_p^n, we associate to σ the linear transformation $e_i \mapsto e_{\sigma(i)}$. Thus G embeds in $GL_n(F_p)$. By the previous example, the group $GL_n(F_p)$ has a p-Sylow subgroup. Hence the same is true for G. □

Theorem 1.9. $C_{qm}^q \equiv m \mod p$, *where q is a power of p and m is relatively prime to p.*

Proof. A typical method to deal with combinatorial identity module p is to consider $R = F_p[t]$. On the one hanc, the coefficient of t^q in $(1+t)^{qm}$ is C_{qm}^q. On the other hand, $(1+t)^q = 1 + t^q$ in R, hence $(1+t)^{qm} = 1 + mt^q + \cdots$. □

Corollary 1.9.1. *Here is a third proof of the first Sylow theorem.*

Miller-Wielandt. Let $|G| = qm$, where q is a power of p, and m is prime to p. Let X be the set of all the subsets of G of cardinality q. We have $|X| = C_{qm}^q$. The above theorem shows that $|X|$ is prime to p. The group G acts on X by left translations. Since $|X|$ is prime to p. there is at least one orbit $\mathcal{O}$ s.t. $|\mathcal{O}|$ is prime to p. Hence $q | |H|$, where H is the stablizier of an element of $\mathcal{O}$, say A.

If $a \in A$, the map $H \to A$ given by $h \mapsto ha$ is injective, hence $|H| \leq |A| = q$. Therefore we have $|H| = q$, and H is a p-Sylow subgroup of G. □

Lemma 1.3. *Let P be a p-group acting on a finite set X. Let X^P be the set of elements of X fixed by P. Then $|X| = \left|X^P\right| \mod p$.*

Proof. Every orbit in $X - X^P$ has order divisible by p. □

Theorem 1.10 (properties of p-Sylow subgroups)**.**
(1) Every p-subgroup of G is contained in a p-Sylow subgroup.
(2) The p-Sylow subgroups of G are conjugate to each other.
(3) The number of p-Sylow subgroups of G is congruent to 1 module p.

Proof of parts (1) and (2). The proof again use the technique of p-group left multiplication.

Let S be a p-Sylow subgroup of G, let P be a p-subgroup of G, and let $X = G/S$. We apply the lemma to P acting on X. Since $|X| \not\equiv 0 \mod p$, we have $\left|X^P\right| \not\equiv 0 \mod p$, hence there exists $x \in X$ fixed by P. The stablizier of x contains P and is also a conjugate of S. Therefore, P is contained in a conjugate gSg^{-1} of S. This proves (1). For (2), notice that the inclusion is an equality since the two groups have the same order. □

Lemma 1.4. *Let S and S' be two p-Sylow subgroups of G. If S' normalizes S, then $S' = S$.*

Proof. S and S' are p-Sylow subgroups of $N_G(S)$. Since S is normal in $N_G(S)$, by (2), S is the unique p-Sylow subgroup of $N_G(S)$. □

Proof of part (3). Let X be the set of p-Sylow subgroups of G, and let S act on X by conjugation. By the above lemma, S is the only element of X that is fixed by all the elements of S. Therefore $\left|X^S\right| = 1$. Thus $|X| \equiv 1 \mod p$. □

Example 1.12. *Recall that, if x is a nonzero integer, $v_l(x)$ is the l-adic valuation of x, i.e., the largest integer m s.t. l^m divides x. For $m > 0$, we have*

$$v_l(m!) = [\frac{m}{l}] + [\frac{m}{l^2}] + [\frac{m}{l^3}] + \cdots$$

As a consequence, we obtain the order of a l-Sylow subgroup of S_m.

1.4 Group Representations

The goal of group representation theory is to study groups via their actions on vector spaces. Consideration of groups acting on sets leads to such important results as the Sylow theorems. By studying actions on vector spaces even more detailed information about a group can be obtained. This is the subject of representation theory.

1.4.1 General Constructions

We only consider representation on a finite-dimensional vector space.

Theorem 1.11. *Let $\varphi : G \to GL(V)$ be a unitary representation of a group. Then φ is either irreducible or decomposable.*

Proof. Suppose φ is not irreducible. Then there is a non-zero proper G-invariant subspace W of U. Its orthogonal complement $W^\perp$ is then also non-zero and $V = W \oplus W^\perp$. So it remains to prove that $W^\perp$ is G-invariant. If $v \in W^\perp$ and $w \in W$, then $\langle \varphi_g(v), w\rangle = \left\langle \varphi_{g^{-1}}\varphi_g(v), \varphi_{g^{-1}}(w)\right\rangle = \left\langle v, \varphi_{g^{-1}}(w)\right\rangle = 0$. We conclude φ is decomposable. □

Theorem 1.12. *Every representation of a finite group G is equivalent to a unitary representation.*

Remark. *This is not true for infinite groups in general.*

Proof. Let $\varphi : G \to GL(V)$ be a representation where $\dim V = n$. Choose a basis B for V, and let $T : V \to \mathbb{C}^n$ be the isomorphism taking coordinates w.r.t. B. Then setting $\rho_g = T\varphi_h T^{-1}$ yields a representation $\rho : G \to GL_n(\mathbb{C})$ equivalent to φ. Let $\langle , \rangle$ be the standard inner product on $\mathbb{C}^n$. We define a new inner product $(,)$ on $\mathbb{C}^n$ using the crucial **averaging trick**:

$$(v, w) = \sum_{g \in G} \langle \rho_g v, \rho_g w\rangle$$

The summation over G, of course, requires that G is finite. Check that it is indeed an inner product, and that the representation is unitary w.r.t. this inner product. □

Corollary 1.12.1. *Let $\varphi : G \to GL(V)$ be a non-zero representation of a finite group. Then φ is either irreducible or decomposable.*

Theorem 1.13 (Maschke)**.** *Every representation of a finite group is completely reducible.*

1.4.2 Character Theory

This subsubsection gets to the heart of group representation theory: the character theory of Frobenius and Schur. The fundamental idea of character theory id to encode a representation $\varphi : G \to GL_n(\mathbb{C})$ of G by a complex-valued function $\chi_\varphi : G \to C$. In other words, we replace a function to an n-dimensional space with a function to a 1-dimensional space.

Lemma 1.5. *Let $T : V \to W$ be in $\hom_G(\varphi, \rho)$. Then $\ker T$ and $\operatorname{Im} T$ are G-invariant.*

Lemma 1.6. *Let $\varphi : G \to GL(V)$ and $\rho : G \to GL(W)$ be representations. Then $\hom_G(\varphi, \rho)$ is a subspace of $\hom(V, W)$.*

Lemma 1.7 (Schur's Lemma)**.** *Let φ, ρ be irreducible representations of G, and $T \in \hom_G(\varphi, \rho)$. Then either T is invertible or $T = 0$.*

Corollary 1.13.1. *Let G be an abelian group. Then any irreducible representation of G has degree one.*

From this point onward, the group G shall always be assumed finite. Let $\varphi : G \to GL_n(\mathbb{C})$ be a representation. Then $\varphi_g = (\varphi_{ij}(g))$ where $\varphi_{ij}(g) \in \mathbb{C}$. Thus there are n^2 functions $\varphi_{ij} : G \to \mathbb{C}$ associated to the degree n representation φ. What can be said about the functions $\varphi_{ij} : G \to \mathbb{C}$ when φ is irreducible and unitary? It turns out that the functions of this sort form an orthogonal basis for $\mathbb{C}^G$.

Definition 1.3 (Group Algebra)**.** Let G be a group and define

$$L(G) = \mathbb{C}^G = \{f | f : G \to \mathbb{C}\}$$

Then $L(G)$ is an inner product space with the inner product given by

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}$$

Theorem 1.14 (Schur Orthogonality Relations)**.** *Suppose that $\varphi : G \to U_n(\mathbb{C})$ and $\rho : G \to U_m(\mathbb{C})$ are inequivalent irreducible unitary representations. Then:*
1. $\langle \varphi_{ij}, \rho_{kl} \rangle = 0$
2. $\langle \varphi_{ij}, \rho_{kl} \rangle = \begin{cases} \frac{1}{n} & i = k \& j = l \\ 0 & else \end{cases}$

We begin the proof with our second usage of the averaging trick.

Lemma 1.8. *Let $\varphi : G \to GL(V)$ and $\rho : G \to GL(W)$ be representations and suppose that $T : V \to W$ is a linear transformation. Then:*
(a) $T^\sharp = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g \in \hom_G(\varphi, \rho)$
(b) If $T \in \hom_G(\varphi, \rho)$, then $T^\sharp = T$
(c) The map $P : \hom(V, W) \to \hom_G(\varphi, \rho)$ defined by $P(T) = T^\sharp$ is an onto linear map.

Lemma 1.9. *Let $\varphi : G \to GL(V)$ and $\rho : G \to GL(W)$ be representations and suppose that $T : V \to W$ is a linear transformation. Then:*
(a) If $\varphi \nsim \rho$, then $T^\sharp = 0$
(b) If $\varphi = \rho$, then $T^\sharp = \frac{\operatorname{tr}(T)}{\deg(\varphi)} I$

Lemma 1.10. *Let $\varphi : G \to U_n(\mathbb{C})$ and $\rho : G \to U_m(\mathbb{C})$ be unitary representations. Let $A = E_{ki} \in M_{mn}(\mathbb{C})$. Then $A^\sharp_{lj} = \langle \varphi_{ij}, \rho_{kl} \rangle$.*

Proof. Since ρ is unitary, $\rho_{g^{-1}} = \rho_g^{-1} = \rho_g^*$. Thus $\rho_{lk}(g^{-1}) = \overline{\rho_{kl}(g)}$. We compute

$$\begin{aligned} A^\sharp_{lj} &= \frac{1}{|G|}\sum_{g\in G}(\rho_{g^{-1}}E_{ki}\varphi_g)_{lj} \\ &= \frac{1}{|G|}\sum_{g\in G}\rho_{lk}(g^{-1})\varphi_{ij}(g) \\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\rho_{kl}(g)}\varphi_{ij}(g) \\ &= \langle \varphi_{ij}, \rho_{kl}\rangle \end{aligned}$$

□

Definition 1.4 (Character)**.** Let $\varphi : G \to GL(V)$ be a representation. The character $\chi_\varphi : G \to \mathbb{C}$ of φ is defined by setting $\chi_\varphi(g) = \operatorname{tr}(\varphi_g)$. The character of an irreducible representation is called an irreducible character.

Lemma 1.11. *Let φ be a representation of G. Then $\chi_\varphi(1) = \deg\varphi$.*

Lemma 1.12. *If φ and ρ are equivalent representations, then $\chi_\varphi = \chi_\rho$.*

Lemma 1.13. *Let φ be a representation of G. Then, $\forall g, h \in G$, the equality $\chi_\varphi(g) = \chi_\varphi(hgh^{-1})$ holds. That is, χ_φ is a class function.*

Definition 1.5 (Class function)**.** A function $f : G \to \mathbb{C}$ is called a class function if $f(g) = f(hgh^{-1})$ for all $g, h \in G$, or equivalently if f is constant on conjugacy classes of G. The space of class functions is denoted by $Z(L(G))$.

Remark. *In particular, characters are class functions.*

Lemma 1.14. *$Z(L(G))$ is a subspace of $L(G)$.*

Next let us compute the dimension of $Z(L(G))$. Let $Cl(G)$ be the set of conjugacy classes of G. Define, for $C \in Cl(G)$, the function $\delta_C : G \to \mathbb{C}$ by

$$\delta_C = \begin{cases} 1 & g \in C \\ 0 & g \notin C \end{cases}$$

Lemma 1.15. *The set $B = \{\delta_C | C \in Cl(G)\}$ is a basis for $Z(L(G))$. Consequently, $\dim Z(L(G)) = |Cl(G)|$*

Theorem 1.15 (First Orthogonality Relations)**.** *Let φ, ρ be irreducible representations of G. Then*

$$\langle \chi_\varphi, \chi_\rho\rangle = \begin{cases} 1 & \varphi \sim \rho \\ 0 & \varphi \not\sim \rho \end{cases}$$

Thus the irreducible characters of G form an orthonormal set of class functions.

Some notation. If V is a vector space, φ is a representation and $m > 0$, then we set

$$mV = \underbrace{V \oplus \cdots \oplus V}_{\times m} \text{ and } m\varphi = \underbrace{\varphi \oplus \cdots \oplus \varphi}_{\times m}$$

Definition 1.6. If $\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$, then m_i is called the multiplicity of $\varphi^{(i)}$ in ρ. If $m_i > 0$, then we say that $\varphi^{(i)}$ is an irreducible constituent of ρ.

Note that it is not clear at the moment if the multiplicity is well-defined because we have not yet established the uniqueness of the decomposition of a representation into irreducibles. To show that it is well defined, we come up with a way to compute the multiplicity directly from the character of ρ. Since the character only depends on the equivalence class, it follows that the multiplicity of $\varphi^{(i)}$ will be the same no matter how we decompose ρ.

Lemma 1.16. *Let $\varphi = \rho \oplus \phi$. Then $\chi_\varphi = \chi_\rho + \chi_\phi$.*

Theorem 1.16. *Let $\varphi^{(1)}, \cdots, \varphi^{(s)}$ be a complete set of representatives of the equivalence classes of irreducible representations of G and let*

$$\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$$

Then $m_i = \left\langle \chi_\rho, \chi_{\varphi^{(i)}} \right\rangle$. Consequently, the decomposition of ρ into irreducible consistuents is unique and ρ is determined up to equivalence by its character.

Proof. By the previous lemma, $\chi_\rho = m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}$. By the first orthogonality relations, we get the desired result. □

Corollary 1.16.1. *A representation ρ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

Next we study a special kind of representation, namely the regular representation.

Theorem 1.17. *The regular representation is a unitary representation of G.*

Theorem 1.18. *The character of the regular representation L is given by*

$$\chi_L(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

Theorem 1.19. *Let L be the regular representation of G. Then holds the decomposition*

$$L \sim d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}$$

Proof. Using the formulas for the character, $\langle \chi_L, \chi_i \rangle = d_i$. □

Corollary 1.19.1. *The formula $|G| = d_1^2 + \cdots + d_s^2$ holds.*

Proof. Evaluate χ_L at 1. □

Theorem 1.20. *The set $B = \left\{ \sqrt{d_k}\varphi_{ij}^{(k)} | 1 \leq k \leq s, 1 \leq i, j \leq d_k \right\}$ is an orthonormal basis for $L(G)$.*

Proof. Compare the two dimensions. □

Theorem 1.21. *The set $\chi_1, \cdots, \chi_s$ is an orthonormal basis for $Z(L(G))$.*

Proof. We show they span $Z(L(G))$. Let $f \in Z(L(G))$, by the averaging trick and $f = \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}$

$$\begin{aligned} f(x) &= \frac{1}{|G|} \sum_{g \in G} f(g^{-1}xg) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}(g^{-1}xg) \\ &= \sum_{i,j,k} c_{ij}^{(k)} \left[\frac{1}{|G|} \sum_{g \in G} \varphi_{g^{-1}}^{(k)} \varphi_x^{(k)} \varphi_g^{(k)} \right]_{ij} \\ &= \sum_{i,j,k} c_{ij}^{(k)} \left[(\varphi_x^{(k)})^\sharp \right]_{ij} \\ &= \sum_{i,j,k} c_{ij}^{(k)} \frac{\operatorname{tr}(\varphi_x^{(k)})}{\deg \varphi^{(k)}} I_{ij} \\ &= \sum_{i,k} c_{ii}^{(k)} \frac{1}{d_k} \chi_k(x) \end{aligned}$$

□

Corollary 1.21.1. *The number of equivalence classes of irreducible representations of G is the number of conjugacy classes of G.*

Proof. $s = \dim Z(L(G)) = |Cl(G)|$ □

Corollary 1.21.2. *A finite group G is abelian if and only if it has $|G|$ equivalence classses of irreducible representations.*

Theorem 1.22 (Second Orthogonality Relations)**.** *Let C, C' be conjugacy classes of G and let $g \in C$ and $h \in C'$. Then*

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} \frac{|G|}{|C|} & C = C' \\ 0 & C \neq C' \end{cases}$$

1.4.3 Burnside's Theorem

Theorem 1.23 (Dimension Theorem)**.** *Let φ be an irreducible representation of G of degree d, then d divides $|G|$.*

Proof. The first orthogonal relations provide $1 = \langle \chi_\varphi, \chi_\rho \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g) \overline{\chi_\varphi(g)}$. Let $C_1, \cdots, C_s$ be the conjugacy classes of G and let chi_i be the value of chi_φ on C_i. Let $h_i = |C_i|$. Then $\frac{|G|}{d} = \sum_{i=1}^{s} \sum_{g \in C_i} \frac{\chi_\varphi(g)}{d} \overline{\chi_\varphi(g)} = \sum_{i=1}^{s} (\frac{h_i}{d} \chi_i) \overline{\chi_i}$. □

Example 1.13. *Let G be a group of order p^2 where p is a prime. Let $d_1, \cdots, d_s$ be the degrees of the irreducible representations of G. Then d_i can be $1, p$ or p^2. Since the trivial representation has degree 1 and $p^2 = |G| = d_1^2 + \cdots + d_s^2$, so all $d_i = 1$ and hence G is abelian.*

Theorem 1.24. *If G' is the commutator subgroup of G, then there is a bijection between degree one representation of G and irreducible representations of the abelian group G/G'. As a result, G has $|G/G'| = [G : G']$ degree one representations.*

Remark. *The number of degree one representations of G divides $|G|$.*

Proof. Every degree one representation of G can be factored through G/G', hence being an irreducible representation of G/G'. The other direct follows from the composition of two maps. □

Example 1.14. *Let p, q be primes with $p < q$ and $q \not\equiv 1 \mod p$. Let $d_1, \cdots, d_s$ be the degrees of the irreducible representations of G. Since $d_i \mid |G|$,$p < q$ and $pq = |G| = d_1^2 + \cdots + d_s^2$, it follows that $d_i = 1$ or $d_i = p$. Let n be the number of degree p representations of G and let m be the number of degree 1 representations of G. Then $pq = m + np^2$. Since m divides pq by the previous lemma, $m \geq 1$ and $p | m$, we must have $m = p$ or $m = pq$. If $m = p$, then $q = 1 + np$, a contradiction. Therefore $m = pq$ and G is abelian.*

Lemma 1.17. *Let G be a group of order n and let C be a conjugacy class of G. Suppose that $\varphi : G \to GL_d(\mathbb{C})$ is an irreducible representation and assume that $h = |C|$ is relatively prime to d. Then either:*
1. $\exists \lambda \in C^*$ s.t. $g \in C \quad \varphi_g = \lambda I$
2. $\forall g \in C \quad \chi_\varphi(g) = 0$

Proof. It suffices to show that if $\varphi_g \neq \lambda I$ for some $g \in C$, then $\chi_\varphi(g) = 0$. We have already known that $\frac{h\chi(g)}{d}$ and $\chi(g)$ are algebraic integers. Since $(d, h) = 1$, we can find integers k, j so that $kh + jd = 1$. Let $\alpha = k(\frac{h\chi(g)}{d}) + j\chi(g) = \frac{\chi(g)}{d}$, then α is an algebraic integer. φ_g is diagonalizable and its eigenvalues $\lambda_1, \cdots, \lambda_d$ are nth-roots of unity, which are not all the same. Thus $|\chi| < d$, and so $|\alpha| < 1$. □

Lemma 1.18. *Let G be a finite non-abelian group. Suppose that there is a conjugacy class $C \neq \{1\}$ of G s.t. $|C| = p^t$ with p prime, $t \geq 0$. Then G is not simple.*

Theorem 1.25 (Burnside)**.** *Let G be a group of order $p^a q^b$ with p, q primes. Then G is not simple unless it is cyclic of prime order.*

2 Rings

2.1 General Constructions

2.2 Concrete Rings

2.2.1 Quaternion Algebra

2.2.2 Möbius Inversion

Definition 2.1 (locally finite poset)**.** A locally finite poset is a partially ordered set P such that for all $x, y \in P$, the interval $[x, y]$ consists of finitely many elements.

Theorem 2.1. *Suppose $(P_1, \leq), \cdots, (P_n, \leq)$ are locally finite posets. Endow $P := \prod_{i=1}^n P_i$ with the order*

$$(x_i)_{i=1}^n \leq (x_i)_{i=1}^n \iff \forall i \quad x_i \leq y_i$$

then P is also a locally finite poset, and its Möbius function is

$$\mu_P(x, y) = \prod_{i=1}^{n} \mu_{P_i}(x_i, y_i)$$

2.2.3 Integrality Properties

Let x be an element of a commutative ring R.

Theorem 2.2 (Z-integral)**.** *TFAE:*
(1) There exist an integer $n \geq 1$, and elements $a_1, \cdots, a_n$ of $\mathbb{Z}$ s.t.:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

(2) The subring $\mathbb{Z}[x]$ of R is a finitely generated $\mathbb{Z}$-module.
(3) The ring $\mathbb{Z}[x]$ is contained in a finitely generated $\mathbb{Z}$-submodule of R.

Remark. *An element having properties (1),(2) and (3) is called integral over $\mathbb{Z}$, or $\mathbb{Z}$-integral; when the ring R is contained in a field of characteristic* 0*, one also says that x is an algebraic integer.*

Theorem 2.3. *The set of Z-integral elements of R is a subring of R.*

Proof. Let x, y be $\mathbb{Z}$-integral elements of R. Then the ring $P = \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}[y]$ is finitely generated over $\mathbb{Z}$. The subring $\mathbb{Z}[x, y]$ of R generated by x and y is isomorphic to a quotient of P, hence finitely generated. Property (3) shows that every element of that ring is $\mathbb{Z}$-integral. Hence $x + y$ and xy are $\mathbb{Z}$-integral. □

Theorem 2.4. *An element of $\mathbb{Q}$ is $\mathbb{Z}$-integral if and only if it belongs to $\mathbb{Z}$.*

Proof. If $x \in \mathbb{Q}$ is $\mathbb{Z}$-integral, it satisfies an eqaution of type:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

If we write $x = \frac{p}{q}$ with (p, q) relatively prime, this eqaution gives

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$$

it implies that p^n is divisible by q. Hence $q = \pm 1$ and $x = \pm p$ belongs to $\mathbb{Z}$. □

Lemma 2.1. *Let $x_1, \cdots, x_n \in \mathbb{C}$ be roots of unity. Suppose that $x = \frac{x_1 + \cdots + x_n}{n}$ is an algebraic integer. Then either $x = 0$, or $x_1 = \cdots = x_n$.*

Proof. Choose a finite Galios extension $K/\mathbb{Q}$, contained in $\mathbb{C}$, and containing all the x_i; let $\Gamma = Gal(K/\mathbb{Q})$. Since x is $\mathbb{Z}$-integral, the same is true of all the $\gamma(x), \gamma \in \Gamma$, and also of their product $X = \prod_{\gamma \in \Gamma} \gamma(x)$. Since X is Γ-invariant, it belongs to $\mathbb{Q}$, then by the previous theorem, it belongs to $\mathbb{Z}$. Each $\gamma(x)$ □

3 Modules

4 Fields

4.1 Finite Fields

Example 4.1. *The number of irreducible polynomials of degree n in $F_p[x]$ is*