Algebra II

Naruki Masuda, transcribed by Hui Sun

April 23, 2025

Contents

Chapter 1

Group Theory

S2013-Q2, S2016-Q1, F2018-Q2, F2001-Q1, F2013-Q1, F2019-Q4

S2005-Q1, F2009-Q1

1.1 Sylow Theorems

We first talk bout semidirect products. Let G be any group, and N, H be subgroups of G.

Definition 1.1. For $\varphi : H \to \mathrm{Aut}(N)$, define $N \rtimes H$ by

(1) $N \rtimes_\varphi H = N \times H$ as a set.

(b) Equipped with the group structure

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \varphi(h_1) n_2, h_1 h_2)$$

The structure $(N \rtimes_\varphi H, \cdot)$ forms a group.

Example 1.1. If N is a normal subgroup of G, and $N \cap H = \{e\}$, and $\varphi : H \to \mathrm{Aut}(N)$ where

$$\varphi : h \mapsto (n \mapsto hnh^{-1})$$

(acting by conjugation), and $G = NH$. Then

$$N \rtimes_\varphi H \to G$$

where

$$(n, h) \mapsto nh$$

is a bijective homomorphism homomorphism. Hence

$$G \cong N \rtimes_\varphi H$$

Next we present some divisibility results.

Proposition 1.1 (Lagrange, Orbit-Stabilizer)**.** We have the following divisibility results:

- Let H be a subgroup of G, let $[G : H]$ denote the number of cosets of H in G, then

$$|G| = |H||[G : H]$$

- Let G be a finite group acting transitively on a finite set A, then for any $a \in A$, we have

$$|\text{Stab}_G(a)| \cdot |O_G(a)| = |G|$$

The class formula is when G acts on itself by conjugation:

Proposition 1.2 (class formula)**.** Let G act on a finite set S, and let Z denote fixed points of this action, then

$$|S| = |Z| + \sum_{a \in A} |O_G(a)|$$

where A includes exactly one element from each nontrivial orbit.

If G acts on itself by conjugation, then

$$|G| = |Z(G)| + \sum_g |[g]| = |Z(G)| + \sum_g \frac{|G|}{|C_G(g)|}$$

where $[g]$ denote the conjugacy class of g, and the sum includes exactly one from each nontrivial conjugacy class in G.

Problem 1.1 (F2019-Q2)**.** 2. Let p, q be two prime numbers such that $p \mid q - 1$. Prove that

(a) there exists an integer $r \not\equiv 1 \mod q$ such that $r^p \equiv 1 \mod q$;

(b) there exists (up to an isomorphism) only one noncommutative group of order pq.

Proof. (a) We want to show that there exists an element $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that

$$r^p \equiv 1 \mod q$$

We can do this because $(\mathbb{Z}/q\mathbb{Z})^\times$ has order $(q-1)$ and $p|(q-1)$. Therefore by Cauchy's theorem, there exists an element of order p in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Let n_p, n_q denote the number of p, q-Sylow subgroups. We see that $n_q|p$ and $n_q \equiv 1 \mod q$, since $p < q$, we must have $n_q = 1$. Now $n_p = 1$ or q by the same reasoning. Suppose $n_q = 1$, let P, Q denote the normal subgroups of order p, q, then

$$G \cong P \times Q$$

by a standard argument (included in the lemma below). Then G is commutative. Since G is noncommutative, we have $n_p = q$. Choose any p-Sylow subgroup P, we know that

$$G \cong Q \rtimes_\theta P$$

where Q is the normal subgroup of order q and $\theta : P \to \text{Aut}(Q) = (\mathbb{Z}/q\mathbb{Z})^\times$. We know either $\theta : 1 \mapsto 1$, is the trivial map which produces a commutative group; or $\theta : 1 \mapsto r$, where $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ is some element of order p.

∎

Lemma 1.1. Let p, q be two primes such that $q \nmid (p-1)$, and N, H has order p, q respectively, suppose that N is normal in G, and $N \cap H = \{e\}$, then

$$G \cong N \times H$$

Proof. We consider the map

$$\psi : N \times H \to G$$

such that

$$(n, h) \mapsto nh$$

We want to show that ψ is a homomorphism and ψ is injective (hence bijective by size argument). It is clearly injective:

$$nh = e \Rightarrow n, h \in N \cap H = \{e\}$$

It suffices to show that ψ is a homomorphism. We see that this implies

$$n_1 n_2 h_1 h_2 = n_1 h_1 n_2 h_2$$

Therefore it suffices to for any $n \in N, h \in H$, one has

$$nh = hn$$

Consider the conjugation action

$$\varphi : H \to \text{Aut}(N)$$

where

$$h \mapsto \left(n \mapsto hnh^{-1}\right)$$

Then we claim that φ is trivial. This is because $\ker(\varphi)$ has size either 1 or q. If it has size q, then the map is trivial; if it has size 1, then H embeds in $\text{Aut}(N)$, however, $|H| = q$, $\text{Aut}(N) = p - 1$, and $q \nmid (p-1)$, hence impossible. This shows that the map is trivial, i.e., for $n \in N, h \in H$,

$$hn = nh$$

as desired. □

Problem 1.2 (F2015-Q1). Prove every group of order 15 is cyclic.

Proof. We will show that any group G of order 15 is isomorphic to

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

For this, using the above lemma, it suffices to show that there is one normal subgroup of order 3 and one normal subgroup of order 5. We repeat the argument above, $n_5 \mid 3$ and $n_5 \equiv 1 \mod 5$, hence $n_5 = 1$. Moreover, $n_3 \mid 5$ and $n_3 \equiv 1 \mod 3$, hence $n_3 = 1$ as well. By the lemma above, we know that

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

hence cyclic as desired. □

Problem 1.3 (S2013-Q2). Let p and q be primes with $p < q$. Let G be a group of order pq. Prove the following statements:

(a) If p does not divide $q-1$ (i.e., $p \nmid q-1$), then G is cyclic.

(b) If p divides $q-1$ (i.e., $p \mid q-1$), then G is either cyclic or isomorphic to a non-abelian group on two generators. Give the presentation of this non-abelian group.

Proof. This question is exactly the same as F19-Q2, we will only outline here.

(a) We have $n_q = 1$, and $n_p \mid q$, hence $n_p = 1$ or q, moreover $n_p \equiv 1 \mod p$. If $n_p = q$, this implies that $p \mid (q-1)$, hence $n_p = 1$. Therefore by the above argument

$$G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$$

(b) If $p \mid (q-1)$, then $n_p = 1$ or q. Hence G is either of the form above or isomorphic to the non-abelian group

$$G = Q \rtimes_\theta P$$

We know from F2019-Q2, the trivial θ defines the abelian, hence cyclic group $G = \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$. And $\theta : 1 \mapsto r$, for some $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ of order p defines a non-abelian group.

not finished, what are the two generators

□

Problem 1.4 (F2007-Q1). Prove that no group of order 148 is simple.

Proof. We note the prime factorization of 148 is

$$148 = 2^2 \cdot 37$$

We see that $n_{37} \mid 4$ and $n_{37} \equiv 1 \mod 37$, therefore $n_{37} = 1$. This shows that there exists a normal subgroup of order 37, i.e., the group is not simple. □

Problem 1.5 (F2017-Q1). Show that there is no simple group of order 30.

Proof. This is slightly more complicated, and we will use a counting argument. Same reasoning as the above. The prime factorization of 30 is as below:

$$30 = 2 \cdot 3 \cdot 5$$

We see $n_5 \mid 6$, and $n_5 \equiv 1 \mod 5$. Unfortunately, n_5 could either be 1 or 6. Now $n_3 \mid 10$, and $n_3 \equiv 1 \mod 3$, unfortunately again n_3 could be 10. However, we argue that $n_3 = 10$ and $n_5 = 6$ cannot happen at the same time. Suppose this is the case, then there are 20 elements of order 2 and 24 elements of order 5, but this is too many! Hence either $n_3 = 1$ or $n_5 = 1$, as desired. □

Problem 1.6 (F2011-Q1)**.**

(a) Let G be a group of order 5046. Show that G cannot be a simple group. You may not appeal to the classification of finite simple groups.

(b) Let p and q be prime numbers. Show that any group of order p^2q is solvable.

Proof. The proof is very similar like above.

(a) The prime factorization of 5049 is as follows:

$$5049 = 2 \cdot 3 \cdot 29^2$$

Hence we see $n_{29} = 1$, i.e., there is a normal subgroup of order 29, therefore not simple.

(b) We will do discussion by cases.

(1) $p > q$. Then $n_p = 1$ or q and $n_p \equiv 1 \mod p$, therefore $n_p = 1$. Let P be the normal subgroup of G of order p^2, we thus have

$$\{e\} \subset P \subset G$$

It is clear that $|G/P| = q$, thus abelian, and $|P| = p^2$ also abelian as well (by the lemma below). This shows that G is solvable.

(2) $p < q$. Then $n_p = 1$ or q, and $n_q = 1$ or p^2. Suppose that $n_q = 1$, let Q denote the normal subgroup of order q, then

$$\{e\} \subset Q \subset G$$

It is clear that Q and G/Q are both abelian. Suppose that $n_q = p^2$ instead, then there are only $p^2q - p^2(q-1) = p^2$ elements of order $\neq q$. Since any p-Sylow subgroup has p^2 elements with order $\neq q$, we must have $n_p = 1$. Hence we are in case (1) again. This shows that G is solvable in either case $n_q = 1, p^2$.

□

Lemma 1.2 (p^2 abelian)**.** Fix prime p, any group of order p^2 is abelian.

Proof. For any nontrivial p group, by the class formula, the center $Z(G)$ is nontrivial, thus the center has order either p or p^2. If it has order p^2, then the group is abelian. If it has order p, then

$$|G/Z(G)| = p$$

is also cyclic, therefore G is abelian (strictly speaking is a contradiction that $|Z(G)| = p$). In either case, we see that G is abelian. □

Problem 1.7. Any p-group is solvable, for any prime p.

Proof. Suppose $|G| = p^r$ for some $r \geq 0$, we will use induction on r. If $r = 0$, then the trivial group is trivally solvable.

- Base case: if $r = 1$, $|G| = p$, then G is cyclic, hence solvable.

- Induction step: suppose that G is solvable for all $|G| = p^k$, where $0 \leq k \leq r-1$. Now we want to show that G of order p^r is solvable. We know G has a nontrivial center, suppose that $|Z(G)| = p^k$, where $1 \leq k \leq r$, then
$$|G/Z(G)| = p^{r-k}, 0 \leq r-k \leq r-1$$
We know any group G is solvable if and only if there exists a sequence of subgroups $G_0, \ldots, G_k$
$$\{e\} = G_0 \subset \cdots \subset G_k = G$$
such that G_{i-1} is normal in G_i and G_i/G_{i-1} is solvable. Therefore we see when $|G| = p^r$,
$$\{e\} \subset Z(G) \subset G$$
has $Z(G)$ solvable, and $G/Z(G)$ also solvable by the induction hypothesis, so we close the induction.

□

Problem 1.8 (S2016-Q1). Classify all groups of order 66, up to isomorphism.

Proof. By $66 = 2 \cdot 3 \cdot 11$, we know $n_{11} = 1$. We claim that there is a normal subgroup isomorphic to $\mathbb{Z}/33\mathbb{Z}$.

1. First we show that there is a subgroup of order 33. Let P_{11} denote the normal subgroup of order 11 and let P_3 denote a 3-Sylow subgroup of G. Then we claim that the following
$$H = \{gh : g \in P_{11}, h \in P_3\}$$
forms a subgroup and is isomorphic to $\mathbb{Z}/33\mathbb{Z}$. By the Lemma 1.1, we see that
$$H \cong \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \frac{\mathbb{Z}}{33\mathbb{Z}}$$

2. Now we show that it is normal. This follows from the following general lemma:

Lemma 1.3. Let p be the smallest prime factor of $|G|$, and let H be a subgroup with index p, then H is normal.

Proof. We will only prove in the case that H is a subgroup of index 2, i.e., $G = H \sqcup (G \setminus H)$. We see for all $g \in G$,
$$gH = Hg$$
since if $g \in H$, then the equality holds; if $g \notin H$, then $gH = G \setminus H$, so is Hg. □

Now since there is a subgroup of order 2, we can write G as a semidirect product
$$G = \frac{\mathbb{Z}}{33\mathbb{Z}} \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$$
The number of nonisomorphic groups will depend on the choice of θ. There are four different choices for $\theta : H \to \operatorname{Aut}\left(\frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) = \frac{\mathbb{Z}}{10\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$
$$\begin{cases} \theta_1 : 1 \mapsto (0,0) \\ \theta_2 : 1 \mapsto (0,1) \\ \theta_3 : 1 \mapsto (5,0) \\ \theta_4 : 1 \mapsto (5,1) \end{cases}$$

what is happening □

Problem 1.9 (S2007-Q2). Prove that no group of order 224 is simple.

Proof. The prime factorization is

$$224 = 2^5 \cdot 7$$

If $n_2 = 1$ or $n_7 = 1$, then we are done; assume that $n_2 = 7$ instead, then we recall G has a nontrivial transitive action on the set of 2-Sylow subgroups, i.e., there is a homomorphism $\varphi : G \to S_7$. We know $\ker(\varphi)$ is a normal subgroup of G. Since the action is nontrivial transitive, we know $\ker(\varphi) \neq G$. If $\ker(\varphi) = \{e\}$, then φ produces an embedding of G into S_7. However, $|G| = 224 \nmid |S_7|$. This shows that $\ker(\varphi)$ is a nontrivial proper normal subgroup of G, concluding that G is not simple. □

Problem 1.10 (F2008-Q1). Show that no group of order 36 is simple.

Proof.

$$36 = 2^2 \cdot 3^3$$

We know $n_2 \mid 9, n_2 \equiv 1 \mod 2$, and $n_3 \mid 4, n_3 \equiv 1 \mod 3$. We know $n_3 = 1$ or 4, suppose that $n_3 = 4$, then there is a nontrivial action of G on the set of 3-Sylow subgroups, i.e.,

$$\varphi : G \to S_4$$

Suppose that G is simple, we know $\ker(\varphi) \neq G$ since the action is nontrivial, by assumption $\ker(\varphi) = \{e\}$, which implies that φ is an embedding, but $|G| = 32 \nmid |S_4|$, which is a contradiction. This implies that G is not simple. □

Problem 1.11 (S2014-Q2). All groups of order less than 60 are solvable, i.e., there exists a sequence of subgroups of G, $G_0, \dots, G_k$ such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian, and

$$1 = G_0 \subset \cdots \subset G_k = G$$

Proof. Groups of order p, pq, p^2, p^2q are solvable.

$$\big\{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23, 25, 26, 28, 29, 30,$$
$$31, 33, 34, 35, 37, 38, 39, 41, 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 55, 57, 58, 59\big\}$$

And any p-group is also solvable.

$$\{8, 16, 27, 32\}$$

The remaining groups are

$$\{24, 36, 40, 42, 48, 54, 56\}$$

24: If $n_2 = 1$ or $n_3 = 1$, then we are done. We see $n_2 = 1$ or 3, consider the action $\varphi : G \to S_3$. We see $\ker(\varphi)$ is a proper normal subgroup of G, this implies that

$$\{e\} \subset \ker(\varphi) \subset G$$

where $|\ker(\varphi)|$ is a known solvable group, hence we are done.

36: Exactly same as above, we assume $n_3 \neq 1$, therefore $n_3 = 4$, the action $\varphi : G \to S_4$ is not injective, hence $\ker(\varphi)$ is again a proper normal subgroup of G that is solvable.

40: We see $n_5 = 1$, therefore

$$\{e\} \subset \mathbb{Z}/5\mathbb{Z} \subset G$$

42: We see $n_7 = 1$.

48: We see $n_2 = 1$ or 3, the the action $\varphi : G \to S_3$ is not injective, hence $\ker(\varphi)$ is a proper normal subgroup of G that is solvable.

54: We see $n_3 = 1$.

56: We know $n_7 = 1$ or 8 and $n_2 = 1$ or 7. The group action argument does not work. We assume $n_7 = 8$, then there can be at most $56 - 8(7-1) = 8$ elements of order $\neq 7$. This shows that $n_2 = 1$. Hence

$$\{e\} \subset P_2 \subset G$$

□

Problem 1.12 (S2012-Q1). Let G be a group of order p^3q^2, where p and q are prime integers. Show that for p sufficiently large and q fixed, G contains a normal subgroup other than $\{1\}$ and G.

Proof. We want to show that there exists a normal group of size p^3, i.e., $n_p = 1$. We know $n_p \mid q^2, n_p \equiv 1 \mod p$. Let p be large enough such that $p > (q^2 - 1)$, then ths forces $n_p = 1$, as desired. □

Problem 1.13 (F2014-Q4).

(a) Let G be a group of order p^2q^2, where p and q are distinct odd primes, with $p > q$. Show that G has a normal subgroup of order p^2.

(b) Can a solvable group contain a non-solvable subgroup? Explain.

Proof. (a) We know $n_p = 1$ or q or q^2, and $n_p \equiv 1 \mod p$. Since $p > q$, we know $n_p \neq q$. It suffices to show that $n_p \neq q^2$: suppose that $n_p = q^2$, then

$$p \mid (q^2 - 1) = (q+1)(q-1)$$

Since p is prime, $p \mid (q+1)$ or $p \mid (q-1)$. The latter impossible since $q < p$. $p \mid (q+1)$ is also impossible because this implies that $q = p + 1$, which implies that q is even, a contradiction.

(b) It is not possible. Suppose G is a solvable group, let H be a subgroup of G, then we know there exists sequence

$$\{e\} = G_0 \subset \cdots \subset G_k = G$$

such that G_i is normal in G_{i+1} and $\frac{G_{i+1}}{G_i}$ is abelian. We define $H_i = G_i \cap H$, then we see H is solvable with sequence $H_0 \subset \ldots H_k$.

□

Problem 1.14 (F2018-Q2). Let G be a group of order 24. Assume that no Sylow subgroup of G is normal in G. Show that G is isomorphic to the symmetric group S_4.

Proof. □

Problem 1.15 (F2001-Q1). Let G be a finite group and let N be a normal subgroup of G such that N and G/N have relatively prime orders.

1. Assume that there exists a subgroup H of G having the same order as G/N. Show that $G = HN$. (Here HN denotes the set $\{xy \mid x \in H, y \in N\}$.)
2. Show that $\phi(N) = N$, for all automorphisms ϕ of G.

Problem 1.16 (S2001-Q1). Let G be a finite group and p the smallest prime number dividing the order $|G|$ of G. Let H be a subgroup of G of index p in G. Show that H is necessarily a normal subgroup of G.

Proof. G has an action on G/H by left multiplication: $\varphi : G \to \text{Aut}(G/H)$ such that

$$\varphi(g)(\bar{g}H) = g\bar{g}H$$

We will show that $H = \ker(\varphi)$. First we see that $\ker(\varphi) \subset H$:

$$\ker(\varphi) = \{g \in G : g\bar{g}H = \bar{g}H : \text{ for all } \bar{g} \in G\}$$

letting $\bar{g} \in H$ we see $g \in \ker(\varphi)$ implies $g \in H$, i.e., $\ker(\varphi) \subset H$.

Now we use a size argument to show $|H| \leq |ker\varphi|$. We note that $\text{im}(\varphi)$ is a subgroup of $\text{Aut}(G/H) = S_p$, thus

$$\frac{|G|}{|\ker(\varphi)|} \text{ divides } p!$$

because $\frac{|G|}{|\ker(\varphi)|}$ also divides $|G|$ and p is the smallest prime that divides p, we must have

$$\frac{|G|}{|\ker(\varphi)|} \text{ divides } p$$

Note that $\frac{|G|}{|H|} = p$, this gives

$$|H| \leq |\ker(\varphi)|$$

which shows $H \subset \ker(\varphi)$, hence $H = \ker(\varphi)$. ∎

(End of Page 5)

1.2 Class Formula, Classification of p-groups

Definition 1.2 (nilpotent group). Let G be a group. Define inductively an increasing sequence $\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$ of subgroups of G as follows: for $i \geq 1$, Z_i is the subgroup of G corresponding to the center of G/Z_{i-1}. One can show that Z_i is normal in G. A group is *nilpotent* if $Z_m = G$ for some m.

Example 1.2.

- p-groups are nilpotent.
- Nilpotent groups are solvable.

Proposition 1.3. We have the following classification of groups of order p, p^2, p^3, for prime p.

- $|G| = p$ implies $G \cong \mathbb{Z}/p\mathbb{Z}$.
- $|G| = p^2$ implies
$$G \cong \frac{\mathbb{Z}}{p^2\mathbb{Z}} \quad \text{or} \quad G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}}$$
- $|G| = p^3$ implies that
$$G \cong \frac{\mathbb{Z}}{p^3\mathbb{Z}} \quad \text{or} \quad G/Z(G) \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}} \quad \text{or} \quad [G, G] = Z(G)$$

Problem 1.17 (S2010-Q1)**.** Let G be a non-abelian group of order p^3, where p is prime. Determine the number of distinct conjugacy classes in G.

Proof. We know G has a nontrivial center, and if $|Z(G)| = p^2$ or p^3, then G is abelian, this shows that $|Z(G)| = p$, now let $g \in G \setminus Z(G)$, then
$$Z(G) \subsetneq Z_g(G) \subsetneq G$$
where $Z(G) \subsetneq Z_g(G)$ because $g \in Z_g(G)$, and $Z_g(G) \subsetneq G$ since $g \notin Z(G)$. This shows that $Z_g(G)$ is a subgroup of order p^2, in other words, the size of the conjugacy class of any $g \in G \setminus Z(G)$ is
$$|[g]| = \left|\frac{G}{Z_g(G)}\right| = p$$
By the class formula,
$$|G| = |Z(G)| + \sum_{a \in A} |[a]|$$
where A contains one a from each nontrivial conjugacy class $[a]$. Thus we have
$$p^3 = p + Np \Rightarrow N = p^2 - 1$$
Every element in $Z(G)$ is its own conjugacy class, thus the total number of conjugacy classes is
$$p^2 + p - 1$$
□

Problem 1.18 (F2013-Q1)**.** Let $p > 2$ be a prime. Classify groups of order p^3 up to isomorphism. The two nonabelian groups of order p^3 (for $p \neq 2$), up to isomorphism, are:
$$\text{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}/(p) \right\}$$
and
$$\begin{aligned} G_p &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a, b \in \mathbb{Z}/(p^2), a \equiv 1 \bmod p \right\} \\ &= \left\{ \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \middle| m, b \in \mathbb{Z}/(p^2) \right\} \end{aligned}$$

Problem 1.19 (F2014-Q5)**.**

(a) Prove that every group of order p^2 (with p prime) is abelian. Then classify such groups up to isomorphism.

(b) Give an example of a non-abelian group of order p^3 for $p = 3$.
Suggestion: Represent the group as a group of matrices.

Proof. (a) See Lemma 1.2. There are two abeliean groups: $\frac{\mathbb{Z}}{p^2\mathbb{Z}}, \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$.

(b) See Problem 1.18.

□

Problem 1.20 (F2019-Q4, S2015-Q3)**.** Find all irreducible representations of a finite p-group over a field of characteristic p.

1.3 Random Problems

Problem 1.21 (F2010-Q1)**.** Let G be a group. Let H be a subset of G that is closed under group multiplication. Assume that $g^2 \in H$ for all $g \in G$. Show that:

- H is a normal subgroup of G
- G/H is abelian

Proof.

- We first show that H is subgroup. It remains to show that if $h \in H$, then $h^{-1} \in H$, we know $(h^{-1})^2 \in H$, thus
$$h(h^{-1})^2 = h^{-1} \in H$$
as desired. Now we show that H is normal: for any $h \in H$, $g \in G$, we want to show $ghg^{-1} \in H$.
$$\begin{aligned} ghg^{-1} &= (gh)^2(gh)^{-1}hg^{-1} \\ &= (gh)^2h^{-1}g^{-1}hg^{-1} \\ &= (gh)^2h^{-1}(g^{-1}h)^2(g^{-1}h)^{-1}g^{-1} \\ &= (gh)^2h^{-1}(g^{-1}h)^2h^{-1} \in H \end{aligned}$$
as desired.
- It suffices to show that for any $g_1, g_2 \in G$, we have
$$g_1g_2H \subset g_2g_1H$$
Take any $h \in H$, we want to show $(g_2g_1)^{-1}g_1g_2h \in H$,
$$\begin{aligned} (g_2g_1)^{-1}g_1g_2h &= (g_2g_1)^{-2}g_2g_1^2g_2h \\ &= (g_2g_1)^{-2}(g_2g_1^2)^2(g_2g_1^2)^{-1}g_2h \\ &= (g_2g_1)^{-2}(g_2g_1^2)^2g_1^{-2}h \in H \end{aligned}$$
as desired.

□

Problem 1.22 (S2014-Q1). Find the number of colorings of the faces of a cube using 3 colors, where two colorings are considered equal if they can be transformed into each other by a rotation of the cube.

[*Hint*: Use Burnside's formula:

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

where a group G acts on a set X, X/G is the set of orbits, and for every $g \in G$, X^g is the fixed subset of g in X.]

Proof. Let X be the set of all possible colorings of the cube (equal cubes allowed), we have $|X| = 3^6$. We notice two things:

1. The group of rotations of a cube is S_4.
2. For $\sigma_1, \sigma_2 \in S_4$ that are conjugates of each other, $|X^{\sigma_1}| = |X^{\sigma_2}$. Therefore for the Burnside's formula becomes

$$|X/S_4| = \frac{1}{|S_4|} \sum_{[\sigma] \text{ conj classes}} |[\sigma]| \cdot |X^\sigma|$$

Now we analyze for each conjugacy class $[\sigma]$, what is $|X^\sigma|$.

- $(1+1+1+1)$, $|[e]| = 1$ and $|X^e| = 3^6$.
- $(1+1+2)$, $|[\sigma_1]| = 6$ and $|X^{\sigma_1}| = 3^3$.
- $(1+3)$, $|[\sigma_2]| = 8$, and $|X^{\sigma_2}| = 3^2$.
- $(2+2)$, $|[\sigma_3]| = 6$, and $|X^{\sigma_3}| = 3^4$.
- (4), $|[\sigma_4]| = 6$, and and $|X^{\sigma_4}| = 3^3$.

Thus combining we get

$$|X/S_4| = \frac{1}{24}\left(3^6 + 6 \cdot 3^3 + 8 \cdot 3^2 + 6 \cdot 3^4 + 6 \cdot 3^3\right) = 57$$

□

Problem 1.23 (S2019-Q4). Let f be a polynomial with n variables and define

$$\mathrm{Sym}(f) = \{\sigma \in S_n \mid f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)\}.$$

1. Prove that $\mathrm{Sym}(f)$ is a subgroup of S_n.
2. Prove that the dihedral group D_4 (the group of symmetries of the square) is isomorphic to $\mathrm{Sym}(x_1x_2 + x_3x_4)$.

Proof.

1. The group S_n acts on the polynomial ring $k[x_1, \ldots, x_n]$, by permuting the x_i to $x_{\sigma(i)}$, and we see that Sym(f) is the centralizer of a fixed element $f \in k[x_1, \ldots, x_n]$, hence is a subgroup.
2. We have a total of 8 elements in Sym$(x_1x_2 + x_3x_4)$:

$$\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$

and we can by drawing a square tha this corresponds to the group D_4.

□

Problem 1.24 (S2011-Q1, F2004-Q1).

(a) Let H be a proper nontrivial subgroup of a finite group G (i.e., $H \neq \{1\}$ and $H \neq G$). Prove that G is not the union of all conjugates of H in G.

(b) Give an example of an infinite group G for which the assertion in part (a) fails.

Proof. (a) If H is normal, then all conjugations of H is equal to H, but $H \subsetneq G$, this G is not not the union of all conjugates of H in G. Now suppose H is not normal, assume the contrary that G is the union of all conjugates of H, then the number of distinct conjugates of H is $[G : N_G(H)]$, hence

$$|G| = [G : N_G(H)] \cdot |H| \iff [G : H] = [G : N_G(H)] \iff [N_G(H) : H] = 1$$

this is a contradiction since H is not normal. Thus G not the union of all conjugates of H in G.

(b) Consider

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{C})$$

It is clear that conjugation of matrices in B do not give matrices with nonzero left bottom entry.

□

Problem 1.25 (S2009-Q1). Let H and K be two solvable subgroups of a group G such that $G = HK$.

1. Show that if either H or K is normal in G, then G is solvable.
2. Give an example where G may not be solvable without the assumption in (a).

Proof. 1. WLOG suppose that H is normal, then the composite map $\varphi = \pi \circ \iota$:

$$K \xrightarrow{\iota} G \xrightarrow{\pi} G/H$$

is surjective, therefore

$$\{e\} \subset H \subset G$$

$G/H \cong K/\ker(\varphi)$ is solvable, hence G is solvable.

2. The smallest nonsolvable group is A_5, we have

$$A_5 = HK$$

where $H = \langle (12345) \rangle, K = A_4 = \{\sigma \in A_5 : \sigma(5) = 5\}$. Now H, K are both solvable, but G is not.

□

Problem 1.26 (F2003-Q1). In a group G, let 1 denote the identity element and let $[x, y] = xyx^{-1}y^{-1}$ denote the commutator of elements $x, y \in G$.

1. Express $[z, xy]x$ in terms of x, $[z, x]$, and $[z, y]$.
2. Prove that if the identity $[[x, y], z] = 1$ holds in G, then the following identities hold in G:

$$[x, yz] = [x, y][x, z] \quad \text{and} \quad [xy, z] = [x, z][y, z].$$

Proof. 1. We have

$$\begin{aligned}[z, xy]x &= zxyz^{-1}y^{-1}x^{-1}x \\ &= zxz^{-1}x^{-1}xzyz^{-1}y^{-1} \\ &= [z, x]x[z, y]\end{aligned}$$

2. The identity $[[x, y], z] = 1$ implies

$$[x, y]z = z[x, y]$$

Therefore using the identity in 1, we have

$$\begin{aligned}[x, yz] &= [x, y]y[x, z]y^{-1} \\ &= [x, y]yy^{-1}[x, z] \\ &= [x, y][x, z]\end{aligned}$$

Similarly

$$\begin{aligned}[xy, z] &= xyzy^{-1}x^{-1}z^{-1} \\ &= xyzy^{-1}z^{-1}zx^{-1}z^{-1} \\ &= x[y, z]x^{-1}[x, z] \\ &= [y, z][x, z] \\ &= [x, z][y, z]\end{aligned}$$

□

Problem 1.27 (S2005-Q1). Let k be a field. Let $G = \mathrm{GL}_n(k)$ be the general linear group, where $n > 0$. Let D be the subgroup of diagonal matrices, and let $N = N_G(D)$ be the normalizer of D in G. Determine the quotient group N/D.

Problem 1.28 (F2009-Q1). Let G be a finite group, and let $\mathrm{Aut}(G)$ be its automorphism group. Consider the group action $\phi\colon \mathrm{Aut}(G) \times G \to G$ defined by $\phi(\sigma, g) = \sigma(g)$. Assume G has exactly two orbits under this action.

1. Determine all such groups G up to isomorphism.
2. For each case from (a), determine when $\mathrm{Aut}(G)$ is solvable.

Problem 1.29 (F2016-Q1). Determine $\mathrm{Aut}(S_3)$.

Proof. Every element $\sigma \in \mathrm{Aut}(S_3)$ must send order 2 elements $\{(12), (23), (13)\}$ to one another, and order 3 elements $\{(123), (132)\}$ to each other. However, σ is determined by how it permutes

$$\{(12), (23), (13)\}$$

Thus every σ is an inner automorphism of the form $\sigma_g(h) = ghg^{-1}$ for $g, h \in S_3$ and g is some transposition. Hence

$$\mathrm{Aut}(S_3) \cong S_3$$

□

Chapter 2

Representation Theory

Theorem 2.1 (Maschke's theorem).

Lemma 2.1 (Schur's Lemma).

Proposition 2.1 (properties of characters).

Proposition 2.2. The character tables for S_3, S_4, A_5, S_5 are as follows:

2.1 Characters

Problem 2.1 (S2008-Q4). Let $V \cong \mathbb{C}^n$ be an n-dimensional complex vector space with standard basis $e_1, \ldots, e_n$. Consider the permutation action $S_n \times V \to V$ defined by:

$$\sigma \cdot e_i = e_{\sigma(i)} \quad \text{for } \sigma \in S_n$$

Decompose V into irreducible $\mathbb{C}[S_n]$-modules.

Problem 2.2 (S2014-Q5). Find the table of characters for S_4.

Problem 2.3 (F2016-Q6). Find a table of characters for the alternating group A_5.

Problem 2.4 (F2015-Q3). Let $G = S_4$ (the symmetric group on four letters).

(a) Prove that G has two non-equivalent irreducible complex representations of dimension 3; call them ρ_1 and ρ_2.

(b) Decompose the tensor product representation $\rho_1 \otimes \rho_2$ into a direct sum of irreducible representations of G.

Problem 2.5 (F2011-Q4). Let $\rho\colon S_3 \to \mathrm{GL}(2,\mathbb{C})$ be a two-dimensional irreducible representation of the symmetric group S_3.

1. Decompose the tensor square $\rho^{\otimes 2}$ into irreducible representations of S_3.
2. Decompose the tensor cube $\rho^{\otimes 3}$ into irreducible representations of S_3.

Problem 2.6 (F2014-Q3). Let $G = S_3$ be the symmetric group on three elements.

(a) Prove that G has an irreducible complex representation of dimension 2 (call it ρ), but none of higher dimension.

(b) Decompose the triple tensor product $\rho \otimes \rho \otimes \rho$ into a direct sum of irreducible representations of G.

Problem 2.7 (S2006-Q6). Let S_4 be the symmetric group on four elements.

1. Give an example of a non-trivial 8-dimensional complex representation of S_4.
2. Show that every 8-dimensional complex representation of S_4 contains a 2-dimensional invariant subspace.

Problem 2.8 (F2007-Q5). Prove that every 5-dimensional complex representation of the alternating group A_4 (the alternating group of degree 4) contains a 1-dimensional invariant subspace.

Problem 2.9 (S2004-Q6). Consider complex representations of a finite group G. Let $\sigma_1, \dots, \sigma_s$ be representatives of the conjugacy classes of G, and let $\chi_1, \dots, \chi_s$ be the irreducible characters of G.

1. Define an inner product on the $\mathbb{C}$-vector space of class functions on G such that $\{\chi_1, \dots, \chi_s\}$ forms an orthonormal basis.
2. Let $A = (a_{ij})$ be the character table matrix of G, where $a_{ij} = \chi_i(\sigma_j)$ for $1 \le i, j \le s$. Prove that A is invertible.

Problem 2.10 (S2018-Q4, S2007-Q5). Is S_4 isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{C})$?

Problem 2.11 (S2010-Q6). Let G be a group of order 24. Using representation theory, prove that $G \neq [G,G]$, where $[G,G]$ denotes the commutator subgroup of G.

Problem 2.12 (F2017-Q6). Let G be a finite group with center $Z(G)$. Show that if G admits a faithful irreducible representation $\rho\colon G \to \mathrm{GL}_n(k)$ for some positive integer $n \in \mathbb{Z}^+$ and some field k, then the center $Z(G)$ is cyclic.

Problem 2.13 (S2005-Q6). Let V be a finite-dimensional vector space over a field k, and let G be a finite group with an irreducible representation $\varphi\colon G \to \mathrm{GL}(V)$. Suppose H is a finite abelian subgroup of $\mathrm{GL}(V)$ contained in the centralizer of $\varphi(G)$. Prove that H must be cyclic.

Problem 2.14 (F2010-Q6). Let G be a non-abelian group of order p^3, where p is prime.

1. Determine the number of isomorphism classes of irreducible complex representations of G, and find their dimensions.
2. Which of these irreducible complex representations are faithful? Justify your answer.

Problem 2.15 (S2011-Q5). Let K be a field, and let $\Phi\colon G \to \mathrm{GL}_n(K)$ be an n-dimensional matrix representation of a group G. Define a G-action on the matrix ring $M_n(K)$ by:

$$(g, A) \mapsto \Phi(g) \cdot A \quad \text{(matrix multiplication)}$$

for $g \in G$ and $A \in M_n(K)$. This action induces a group homomorphism $\Psi\colon G \to \mathrm{GL}(M_n(K))$. Express the character χ_Ψ of Ψ in terms of χ_Φ (the character of Φ).

Problem 2.16 (S2015-Q5). Prove that a tensor product of irreducible representations over an algebraically closed field is irreducible.

Problem 2.17 (S2001-Q3). Calculate the complete character table for $\mathbb{Z}/3\mathbb{Z} \times S_3$, where S_3 is the symmetric group in 3 letters.

2.2 Induced representations

Problem 2.18 (S2009-Q6). Let $G = S_4$ and consider the subgroup $H = \langle (1\,2), (3\,4) \rangle$.

(a) Determine the number of irreducible complex characters of H.

(b) Choose a non-trivial irreducible character ψ of H over $\mathbb{C}$ satisfying $\psi((1\,2)(3\,4)) = -1$. Compute the values of the induced character $\mathrm{ind}_H^G(\psi)$ on all conjugacy classes of G, and express it as a sum of irreducible characters of G.

2.3 Frobenius Reciprocity

Problem 2.19 (S2017-Q6). Let G be a finite group and H an abelian subgroup. Show that every irreducible representation of G over $\mathbb{C}$ has dimension $\leq [G : H]$.

Problem 2.20 (S2008-Q6). Give an example of non-isomorphic finite groups with same character table. Construct the character table in detail.

Problem 2.21 (S2012-Q4). Let Q be the quaternion group with presentation:

$$Q = \langle t, s_i, s_j, s_k \mid t^2 = 1,\ s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t \rangle.$$

(a) Find four non-isomorphic 1-dimensional real representations of Q.

(b) Prove that the natural embedding $\rho\colon Q \to \mathbb{H}$ given by:

$$\rho(t) = -1, \quad \rho(s_i) = i, \quad \rho(s_j) = j, \quad \rho(s_k) = k$$

defines an irreducible 4-dimensional real representation of Q, where $\mathbb{H}$ is the algebra of real quaternions.

(c) Classify all irreducible complex representations of Q up to isomorphism.

Problem 2.22 (F2004-Q6). Let D_8 be the dihedral group of order 8, with presentation:

$$D_8 = \langle r, s \mid r^4 = 1 = s^2,\ rs = sr^{-1} \rangle.$$

1. Determine all conjugacy classes of D_8.
2. Find the commutator subgroup D_8' of D_8 and determine the number of distinct degree-1 (linear) characters of D_8.
3. Construct the complete complex character table of D_8.

Problem 2.23 (F2000-Q7). Let D_{10} be the dihedral group of order 10, with presentation:

$$D_{10} = \langle r, s \mid r^5 = 1 = s^2,\ rs = sr^{-1} \rangle.$$

1. Determine all conjugacy classes of D_{10}.
2. Compute the commutator subgroup D_{10}' of D_{10}.
3. Prove that $D_{10}/D_{10}' \cong \mathbb{Z}/2\mathbb{Z}$ and deduce that D_{10} has exactly two distinct degree-1 characters.
4. Construct the complete complex character table of D_{10}.