SOLUTIONS TO HOMEWORK

BOWEN LIU

0. Introduction

We will omit proofs which are already shown in the textbook or quite trivial.

Contents

1. Homework 1

1.1. **Sol for 2.1.**

1 Omit.

2 Here we prove by induction: It's clear for $n = 1$; If we have already proven for $n < k$, then for $n = k$, we have

$$\begin{aligned}(ab)^k &= (ab)^{k-1}(ab)\\ &= a^{k-1}b^{k-1}ab\\ &= a^{k-1}ab^{k-1}b\\ &= a^kb^k\end{aligned}$$

If we want to find $a, b \in G$ such that $(ab)^2 \neq a^2b^2$, it suffices to find a, b such that $ab \neq ba$, since you can cancel a, b from two sides of $(ab)^2 \neq a^2b^2$. It's easy to find such elements in a non-abelian group, and note that a quite simply non-abelian group is $\mathrm{GL}_2(\mathbb{R})$, that is group consists of 2×2 real matrices which are invertible. For example:

$$a = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad b = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

3 Omit.

4 Omit.

5 Note that

$$\begin{aligned}ab &= (ab)^{-1}\\ &= b^{-1}a^{-1}\\ &= ba\end{aligned}$$

6 Omit

8 If for all $a \neq e$, we have $a^{-1} \neq a$, then the order of G must be odd, a contradiction.

1.2. **Sol for 2.2.**

1 Let H, K be two subgroups of G such that one don't contain another, take $x \in H - K, y \in K - H$, then $xy \notin H \cup K$. Indeed, if $xy \in H$, then $y = x^{-1}xy \in H$, a contradiction, the same contradiction holds for $xy \in K$.

Remark 1.2.1. In fact, you can use this exercise to give a neat proof of Hua's semi-homomorphism theorem[1] when we learn ring theory.

2 Omit.

3 The following proof is wrong, since G may not be a finite group.

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]$$

[1]A semi-homomorphism of ring must be a homomorphism or anti-homomorphism.

4 There is already a concrete proof in textbook, here we give a more abstract method: It's easy to check H is a subgroup if and only if $H^2 = H, H^{-1} = H, H \neq \varnothing$. Then If HK is a subgroup, then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$; Conversely,
(a) $(HK)(HK) = H(KH)K = H^2K^2 = HK$
(b) $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$;
(c) Of course $HK \neq \varnothing$
This shows HK is a subgroup.

5 Omit.

Remark 1.2.2. For arbitrary subgroups H, K of G(Note that we don't assume they're finite), consider the following group action

$$\begin{aligned} H \times G/K &\to G/K \\ (h, gK) &\mapsto hgK \end{aligned}$$

Then the orbit of $K \in G/K$ is exactly HK/K, and stabilizer of K is $H \cap K$, which implies

$$\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}$$

6 Note that

$$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K]$$

Bonus 1.2.1. Show that $[G : H \cap K] = [G : H][G : K]$ if and only if $G = HK$.

7 Note that order of every element of H divides $|H|$, and similar for K, thus any element $x \in H \cap K$ must have order dividing $(|H|, |K|) = 1$, which implies $x = e$.

8 Omit.

12 Omit.

1.3. **Sol for 2.3.**

1. It suffices to show $NH = HN$. Note that H is a normal subgroup, thus we have $NHN^{-1} = H$, which implies $HN = HN$.
2. Note that for every $g \in G$, gHg^{-1} is a subgroup with order m, but there is only one subgroup with order m, this shows $gHg^{-1} = H$ for any $g \in G$, that is H is a normal subgroup.

2. Homework 2

2.1. Sol for 2.3.

4 It's clear $xyx^{-1}y^{-1} \in N \cap H$.

Bonus 2.1.1. In a group G, we always use $[x, y]$ to denote $xyx^{-1}y^{-1}, x, y \in G$, which is somtimes called a commutator. You can think that $[x, y]$ measures the failure of x and y to commute with each other. The subgroup generated by $[x, y]$ is called the derived subgroup, which is denoted by $[G, G]$. Prove:
(a) $[G, G]$ is a normal subgroup of G;
(b) $G/[G, G]$ is the largest abelian quotient group.

5 Omit.
6 Omit.

Bonus 2.1.2. Try to use this exercise to show a group with order 4 must be abelian. Hint: It suffices to show G has non trivial center.

Remark 2.1.1. Later you can use class equation to show any group with order p^2 must have a non trivial center, so proof in here can also show a group with order p^2 must be abelian.

7 Consider the image of x in G/N.
8 From (4), we can see for any $x, y \in G$ and $n \in N$, we have

$$nxyx^{-1}y^{-1} = xyx^{-1}y^{-1}n$$

which implies n commute with any element taking form xy. Take $y = e$, then we obtain $n \in C(G)$.
9 There are too many ways to define dihedral group, we use the following one:

Definition 2.1.1 (dihedral group)**.** Dihedral group $D_n, n > 2$ is defined as follows

$$D_n = \{r, s \mid r^n = e, s^2 = e, srs^{-1} = r^{-1}\}$$

In this way, you can see the following things:
(a) You can think D_n characterizes the symmetries of a regular n-polygon: r means rotation by $\frac{2\pi}{n}$ angles and s means reflection with respect to some axis. More explicitly, you can write them as matrices as

$$r = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(b) We need $n > 2$ in the definition, since there is no 2-gon;
(c) It's easy to see it's non abelian, since $srs^{-1}r^{-1} = r^{n-2} \neq e$;
In order to do some concrete computation, we need a more explicit expression.

Bonus 2.1.3. Show that every element of D_n is uniquely expressible as $s^i r^j$ where $0 \leq i \leq 1$ and $0 \leq j \leq n - 1$.

If you have solved the bonus, you will find my definition is exactly the ugly one in textbook. In computation of D_n, we always divide into two cases. For example, if we want to see an element x whether lie in center of D_n or not, it suffices to use arbitrary element to conjugate x.

(a) $x = r^a s$. Then use $r^b s$ to conjugate it, we have
$$(r^b s)r^a s(sr^{-b}) = r^b sr^a r^{-b} = r^{2b-a}s$$
In general this element depending on b, so an element taking form $r^a s$ won't lie in center.

(b) $x = r^a$. Then use $r^b s$ to conjugate it, we have
$$(r^b s)r^a(sr^{-b}) = r^{-a}$$
and it's clear r^a commutes with r^b.

So the only possible element in center of D_n takes the form r^a such that $r^a = r^{-a} = r^{n-a}$. We can only find such non trivial element in case that n is even, and only one, that is $r^{\frac{n}{2}}$. In conclusion,
$$C(D_n) = \begin{cases} \{1\}, & n \text{ is odd} \\ \mathbb{Z}_2, & n \text{ is even} \end{cases}$$

Bonus 2.1.4. Find all finite subgroups of O(2), that is group of 2×2 orthogonal groups.

11 Omit.

12 In fact, you can see the hallmark of the proof in textbook is that you can always solve equation $w = z^n$ in $\mathbb{C}^*$.

Definition 2.1.2 (divisible group)**.** A group G is divisible if for every $x \in G$ and positive integer n there is $y \in G$ such that $y^n = x$.

Bonus 2.1.5. Show:

(a) A quotient of a divisible group is divisible;

(b) Any finite divisible group is trivial;

(c) Show any finite index proper subgroup of $(\mathbb{Q}, +)$ is trivial.

2.2. **Sol for 2.4.**

1 Omit.

2 Omit.

3 Omit.

4 Omit.

5 Omit.

6 It's clear to see N has index 2 thus it's normal.

Bonus 2.2.1. You know that a normal subgroup must be a union of many conjugacy classes. So try to write down all conjugacy classes of D_n, and write N as a union of conjugacy classes.

Remark 2.2.1. You may wonder why I ask you to do such a boring thing, here is two things I want to explain:

1. A group without any non trivial normal subgroup is called simple group. Of course there is a smart way to show A_5 is a simple group, but you can show A_5 is simple by counting its conjugacy classes and see there is no non trivial subgroup can be a union of these conjugacy classes(Lagrange theorem may help). There is an easy way to count conjugacy classes of A_5, so it's a quick way.

   Bonus 2.2.2. Show A_5 is simple by counting its conjugacy classes.

2. Later maybe I will show you a little group reprensentation theory using dihedral groups. A fact is that the number of irreducible representations equals to the number of conjugacy classes.

7 Omit.

Remark 2.2.2. If you know a little about Lie group and Lie algebra, you will know this exercise can be used to show the Lie algebra of a abelian Lie group is also abelian. The hallmark of the proof is to note that inversion map $\iota(g) = g^{-1}$ is a group homomorphism and check Lie algebra homomorphism induced by ι is $-\mathrm{id}$.

Bonus 2.2.3. Show Lie algebra of an abelian Lie group is still abelian.

8 Note that there is a one to one correspondence between normal subgroup of G/H and normal subgroup of G containing H.
9 Omit.
12 Textbook show that φ is surjective, here I try to show φ is injective: If $x^m = e$, thus order of x divides m, but we also have order of x divides the order of group, that is n, thus order of x divides $(m, n) = 1$, which implies $x = e$.
13 Omit.
14 Omit.

2.3. **Sol for 2.5.**

1 Omit.
2 It suffices to check any subgroup generated by two elements is cyclic, that is generated by one element: If $H = \langle a, b\rangle$, you can always find $r \in \mathbb{Q}$ such that $a = ra'$, $b = rb'$, thus $H = \langle a, b\rangle \subseteq \langle r\rangle$, thus H is cyclic, since it's a subgroup of cyclic subgroup.

Bonus 2.3.1. Use this exercise to show $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q} \times \mathbb{Q}, +)$. Hint: Find a finitely generated subgroup of $\mathbb{Q} \times \mathbb{Q}$ which is not cyclic.

3 If G is a cyclic group $\langle a\rangle$ of order p^n, where p is prime, it's clear all subgroups of G is a totally ordered set, since any subgroup of G takes form $\langle a^k\rangle$, where k divides p^n. Conversely, list all proper subgroups of G as follows
$$\{e\} \leq H_1 \leq \cdots \leq H_m \leq G$$

If $|H_m| = p^k$ with $k < n$, take $g \in G - H_m$, then we must have $\langle g \rangle = G$, since $\langle g \rangle \neq H_m$, which implies G is cyclic.

Remark 2.3.1. It's a quite interesting phenomenon, that is property of the whole group is characterized by subgroups, and this exercise is not the only case, for example, here is a generalization:

Bonus 2.3.2. For every finite group G of order n, the following statements are equivalent:
(a) G is cyclic.
(b) For every divisor d of n, G has at most one subgroup of order d.

Later we will see other examples, when we learn more properties about group.

4 If $\varphi : G \to H$ is a group homomorphism, then I claim $o(\varphi(x))$ divides $o(x)$. Indeed, $o(x) = m$ implies $e_H = \varphi(e_G) = \varphi(x^m) = \varphi(x)^m$. So if φ is a group isomorphism, we have $o(x)$ divides $o(\varphi(x))$ and $o(\varphi(x))$ divides $o(x)$, thus φ preserves order of elements. It's clear group homomorphism won't preserve, just take trivial homomorphism $\varphi : G \to \{e\}$, all elements are mapped to an element of order 1.

3. Homework 3

3.1. **Sol for 2.5.**

5 Omit;

6 Given a surjective group homomorphism $\varphi : H \to G$ between cyclic groups, where generator of H is denoted by h. To see φ is an isomorphism, it suffices to check $\ker\varphi$ is trivial: Note that $\ker\varphi$ is a subgroup of H, then it's generated by h^m for some $m \in \mathbb{N}$. If $m \neq 0$, then $G \cong H/\ker\varphi = \mathbb{Z}_m$, a contradiction. So $\ker\varphi$ is trivial.

7 Omit;

8 Omit;

9 Given a group homomorphism $\varphi : H \to G$, where H is finite and G is infinite. By exercise 4 of 2.5, we have order $\varphi(x)$ divides order of x, which implies $\varphi(x) = e_G$, otherwise order of $\varphi(x)$ will be infinite.

3.2. **Sol for 2.6.**

1 Omit;

2 Omit;

3 Omit;

4 Omit;

5 Omit;

6 Omit;

7 Omit;

8 It suffices to show that every element $\sigma \in S_p$ with order p has form $(1, i_1, \dots, i_{p-1})$, where $i_1, \dots, i_{p-1}$ is a permutation of $2, 3, \dots, p$, thus there are exactly $(p-1)!$ elements with order p.

It's clear to see, if cycle type of σ is $(m_1, \dots, m_k)$, then the order of σ is $\operatorname{lcm}(m_1, \dots, m_k)$. So if order of σ is prime p, then its cycle type must be (p), since only divisors of p is $1, p$. Thus $\sigma = (1, i_1, \dots, i_{i-1})$.

Bonus 3.2.1. Use this exercise to show the number of Sylow p subgroups of S_p is $(p-2)!$.

9 Omit;

10 Since cases $n = 1, 2$ are trivial, let's assume $n \geq 3$. Note that A_n is generated by 3-cycles if $n \geq 3$, and each 3-cycle (abc) is a commutator, since

$$(abc) = (ab)(ac)(ab)(ac)$$

Thus $A_n \subseteq [S_n, S_n]$. Conversely, since $S_n/A_n = \mathbb{Z}_2$ is abelian, then by Bonus 2.1.1 we have $[S_n, S_n] \subseteq A_n$. Thus we have $A_n = [S_n, S_n]$.

11 Let H be a subgroup of A_4 with order 6, then choose a 3-cycle x not in H, and consists the cosets H, xH, x^2H in A_4/H. Since A_4/H is a group of order 2, two of the cosets must be equal. But H and xH are distinct, so x^2H must be equal to one of them.

(a) If $x^2H = H$, then $x^2 = x^{-1} \in H$, so $x \in H$, a contradiction;

(b) If $x^2H = xH$, then $x \in H$, a contradiction.

So H doesn't exist.

12 Omit;

13 Let H be a normal subgroup of S_n, then $H \cap A_n$ is a normal subgroup of A_n, thus
(a) $H \cap A_n = A_n$;
(b) $H \cap A_n = \{e\}$.
For the first case, we must have $H = S_n$, since there is no subgroup between $A_n \subset S_n$. For the second case, note that $A_n = [S_n, S_n]$, thus by exercise 8 of 2.3 we have $H \subset Z(S_n) = \{e\}$.

14 Consider isomorphism

$$r \mapsto \sigma$$

$$s \mapsto \tau$$

3.3. **Sol for 2.7.**

2 Consider G acts on the G/H, and denote group homomorphism corresponding to this action by $\varphi : G \to S_n$. Then consider normal subgroup $K = \ker \varphi$, we have $[G : K] \mid n!$. In particular, if $|G| \nmid n!$, then $|K| \neq 1$, which implies K is nontrivial (It's trivial $K \neq G$).

5 It's clear $|G| \nmid p!$, by exercise 2 there exists a nontrivial normal subgroup $K \subseteq H$ such that $[G : K] \mid p!$, which implies $[G : K] = p$. But

$$p = [G : K] = [G : H][H : K] = p[H : K]$$

so we have $K = H$.

7 By the same proof of exercise 2, it's clear to see there exists a normal subgroup N contained in H such that $[G : N] \mid n! < \infty$, thus

$$[H : N] \leq [G : N] < \infty$$

8 Omit;

4. Homework 4

4.1. **Sol for 2.7.**

1 Omit;

3 (6) of Example 8 in textbook implies

$$\sum_{x \in \operatorname{Conj} G} \frac{1}{|Gx|} = 1$$

where $\operatorname{Conj} G$ is the set of conjugacy classes of G and Gx is the orbit of the action. So here we consider the conjugate action of G on itself and Gx is exactly the stabilizer of x. This gives the desired equation.

4 (a) Recall that you can write any normal subgroup N as a union of conjugacy classes, and for p-group, the number of elements in any conjugacy classes is exactly powers of p (since they're stabilizers of conjugate action). Since N contains at least one conjugacy classes with one element (the class of identity), and $|N|$ is also power of p, so it must contain other classes with just one element which must be classes of centeral elements of G.

(b) If H is a proper subgroup of G, consider right action of H on cosets G/H. It's clear $|G/H|$ is power of p, and there is at least one orbit with one element (the orbit consists of H), so there must be other orbits with one element, for example Hg, that is $Hgh = Hg$ for arbitrary $h \in H$, which implies $g^{-1}Hg = H$, thus $g \in N(H) \backslash H$, which implies $H \subsetneq N(H)$.

Remark 4.1.1. The ideals of proof for (a) and (b) are same.

(c) Note that H is a proper subgroup of G, by (b) we have $H \subsetneq N(H)$, which implies $N(H) = G$, thus H is normal.

Remark 4.1.2. Of course you can use exercise 5 of 2.7, since you've proven it.

6 If $[G : H] = n < \infty$ and $|H| = k$, there are at most n distinct conjugates of H. Since the identity element is in all of the conjugacy classes, the union of conjugates of H has at most

$$n(k-1) + 1 = nk - n + 1$$

elements. If $n = 1$, that is H is normal, it's clear the union of conjugates of H can't be the whole group since H is proper subgroup. So we must have

$$\Big|\bigcup_{g \in G} gHg^{-1}\Big| \leq nk - (n-1) < nk = |G|$$

This completes the proof.

Bonus 4.1.1. Show that:

1. Only assume H is finite index, prove above exercise again;

2. Give an example to show if H is infinite index, then the conjugates of H may equal to the whole group. Hint: Recall what does Jordan normal form tell you?

9 Omit;
10 If $n \geq 3$, then for arbitrary i, j, you can pick $k \neq i, j$ and then $(ik)(ij) \in A_n$ translate i to j.

Definition 4.1.1 (2-transitive)**.** A group G acts 2-transitive on a set S if it acts transitively on the set

$$\{(x, y) \in S \times S \mid x \neq y\}$$

Remark 4.1.3. Similarly you can define what is k-transitive for $k \in \mathbb{Z}_{\geq 0}$.

Bonus 4.1.2. Show that:
1. S_n is n-transitive;
2. A_n is $n-2$-transitive, $n \geq 3$.

11 Omit;
12 Omit;
13 I think it's the same as exercise 6.
14 Omit;
15 Given a subgroup H with index 3, then by exercise 2 of 2.7 we know that there exists a normal subgroup K contained in H such that $[G : K] \mid 3! = 1 \times 2 \times 3$. Thus $[G : K]$ may equal 3 or 6. It suffices to check $[G : K] \neq 6$. If $[G : K] = 6$, then $G/K \cong S_3$ and there exists a subgroup H/K with order 2 of G/K since S_3 do, which implies

$$[G : H] = [G/K : H/K] = 2$$

a contradiction.

4.2. Sol for 2.8.

1 Note that $|S_4| = 24 = 2^3 \times 3$, so there are 3-sylow subgroups and 2-sylow subgroups of S_4:
(a) The number of 3-sylow subgroups may be 1 or 4. Note that elements in S_4 with order 3 must have form (123), and there are 8 of them. As each of these is contained in at least one 3-sylow subgroup, so there won't be only one 3-sylow subgroups.
(b) The number of 2-sylow subgroups may be 1 or 3. Note that elements in S_4 with order 4 must have form (1234) and there are 6 of them, elements in S_4 with order 2 have form (12) or (12)(34) and there are both 6 of them. As each of these is contained in at least one 2-sylow subgroup, so there won't be only one 2-sylow subgroups.

Remark 4.2.1. This counting method is quite useful in showing a subgroup is not normal or not.

Bonus 4.2.1. Consider $\mathrm{SL}(2, \mathbb{F}_3)$, that is special linear group of 2×2 over $\mathbb{F}_3$, it's also a group with order 24. Show that there is only one 2-sylow subgroup. Hint: Firstly you need to show there are four 3-sylow subgroups, and assume there are three 2-sylow subgroups, you will get toooo many elements.

Bonus 4.2.2. For a group G with order pqr, where $p < q < r$ are distinct prime numbers, show r-sylow subgroup must be normal.

Proof. (Sketch). Firstly show there is at least a normal subgroup by counting method, if r-sylow subgroup is normal, then we're done. So we may assume p-sylow subgroup P is normal, then consider G/P, a group of order qr, which contains a normal r-sylow subgroup, then G contains a normal subgroup H of order pr by correspondence. The r-sylow subgroup of G must be r-sylow subgroup of H, which implies the r-sylow subgroup of G is unique. □

Bonus 4.2.3. For a group with order $p_1 p_2 \dots p_r$ where $p_1 < p_2 < \cdots < p_r$ are distinct prime numbers, show there is only one p_r-sylow subgroup. Hint: Prove by induction.

2 Omit;
3 Omit;
4 By example 4 in textbook you can see there are only two groups with order 6, one is $\mathbb{Z}_6$ and the other one is S_3.
5 It suffices to check there is an element with order $p_1 p_2 \dots p_t$. For each $1 \leq i \leq t$, there exists at least a p_i-sylow subgroup, which must be a cyclic subgroup generated by a_i. Since G is abelian then for arbitrary $i \neq j$ we have $a_i a_j = a_j a_i$. Then by exercise 10 of 2.2 we have $a_1 a_2 \dots a_t$ is an element with desired order.

Remark 4.2.2. If you know the structure of finite abelian group, it's a trivial result.

6 Omit;
7 Omit;
8 Firstly, it's clear to see 11-sylow subgroup P_{11} is normal, since $231 = 11 \times 7 \times 3$. In order to show 11-sylow subgroup P_{11} is contained in center, let's consider conjugate action of G on P_{11}, which induces a group homomorphism
$$\varphi : G \to \mathrm{Aut}(P_{11}) = \mathbb{Z}_{10}$$
Thus we obtain an isomorphism
$$G/\ker\varphi \cong H$$
where H is a subgroup of $\mathbb{Z}_{10}$. However, subgroups of $\mathbb{Z}_{10}$ must have order $10, 5, 2, 1$, and there is no subgroup of G with index $10, 5, 2$, which implies $|G/\ker\varphi| = 1$, that is P_{11} is contained in center of G.
9 Omit;

10 If you have already solved Bonus 4.2.2, then it's clear 5-sylow subgroup P_5 is normal, thus P_5P_3 is a subgroup of G, where P_3 is 3-sylow subgroup. Furthermore, P_5P_3 is a normal subgroup of G since its index is 2. However, it's clear that 3-sylow subgroup of P_5P_3 is normal, thus 3-sylow subgroup of G is also normal since P_5P_3 is normal in G.

11 Note that $72 = 2^3 \times 3^2$, so the number of 3-sylow subgroup of G, denoted by n_3, may be 1 or 4.
   (a) If $n_3 = 1$, there is nothing to prove, since 3-sylow subgroup is normal;
   (b) If $n_3 = 4$, let's consider G acts on the set of 3-sylow subgroups by conjugate action, which induces a group homomorphism
$$\psi : G \to S_4$$
   Note that $|G/\ker\varphi|$ divides $|S_4| = 2^3 \times 3$, so we must have 3 divides $\ker\varphi$, which implies $\ker f \neq \{e\}$. Furthermore, $\ker\varphi \neq G$, otherwise there will only be one 3-sylow subgroup, a contradiction. Thus in this case $\ker\varphi$ is a non-trivial normal subgroup of G.

12 I think there is one more condition required: G is not abelian.

14 Omit;

4.3. **Sol for 2.9.** I think maybe most of you have encountered quite similar exercises when you're learning (inner) product of vector space, since vector space is an abelian group together with a field action on it in fact.

1 Omit;

2 Omit;

3 Omit;

4 Omit;

6 Omit;

8 It suffices to check for any i, we have $N_i \cap N_1 \dots N_{i-1}N_{i+1} \dots N_n = \{e\}$. Indeed,
$$\begin{aligned} |G| &= |N_iN_1N_2 \dots N_{i-1}N_{i+1} \dots N_n| \\ &= \frac{|N_i||N_1 \dots N_{i-1}N_{i+1} \dots N_n|}{|N_i \cap N_1 \dots N_{i-1}N_{i+1} \dots N_n|} \\ &= \frac{|G|}{|N_i \cap N_1 \dots N_{i-1}N_{i+1} \dots N_n|} \end{aligned}$$

9 Omit;

10 Firstly we need to show G is abelian: for any $a, b \in G$, we have
$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$
   since any element of G has order two. Then take arbitrary $a_1 \in G$ and let $N_1 = \langle a_1 \rangle$, if $N_1 \subsetneq G$, then choose $a_2 \in G - N_1$ and let $N_2 = \langle a_2 \rangle$. Repeat this process to construct N_i untill $N_1N_2 \dots N_{i-1} = G$. It's clear such $N_1, \dots, N_n$ for some n satisfies the condition of exercise 9, this shows G is product of some $\mathbb{Z}_2$.

11 Omit;

14 Omit;

5. Homework 5

5.1. **Sol for 2.10.**

1 Omit;
2 Omit;
3 Omit;
4 Omit;
5 Omit;
6 Omit;
7 Omit;
8&9

Proposition 5.1.1. For any $n \in \mathbb{Z}_{>1}$, we have

$$\operatorname{Aut} \mathbb{Z}_n = (\mathbb{Z}_n)^\times$$

where $(\mathbb{Z}_n)^\times$ is the multiplicative group of $\mathbb{Z}_n$.

Proof. Let x be a generator of $\mathbb{Z}_n$, then any automorphism φ of $\mathbb{Z}_n$ is determined by $\varphi(x)$. Furthermore $\varphi(x) = x^k$ must generate the whole group $\mathbb{Z}_n$, which implies $\gcd(k, n) = 1$, that is $x^k \in (\mathbb{Z}_n)^\times$, that is $\operatorname{Aut} \mathbb{Z}_n \subseteq (\mathbb{Z}_n)^\times$; Conversely, given an element in $(\mathbb{Z}_n)^\times$, it's easy to construct an automorphism.

Thus we obtain a one to one correspondence between $\operatorname{Aut} \mathbb{Z}_n$ and $(\mathbb{Z}_n)^\times$. Furthermore, it's an group isomorphism. □

Corollary 5.1.1. For prime p, we have

$$\operatorname{Aut} \mathbb{Z}_p = \mathbb{Z}_{p-1}$$

Proof. It's clear

$$(\mathbb{Z}_p)^\times = \mathbb{Z}_{p-1}$$

□

Corollary 5.1.2. For groups with 2-power order, we have
1. $\operatorname{Aut} \mathbb{Z}_4 = \mathbb{Z}_2$;
2. $\operatorname{Aut} \mathbb{Z}_8 = \mathbb{Z}_2 \times \mathbb{Z}_2$;
3. $\operatorname{Aut} \mathbb{Z}_{2^n} = \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}, n \geq 4$.

Proof. It's clear $\operatorname{Aut} \mathbb{Z}_4 = \mathbb{Z}_2$, since there are only two elements in $(\mathbb{Z}_4)^\times$, which can be seen from $\phi(4) = 2$, where ϕ is Euler function. Similarly you can see there are four elements in $\operatorname{Aut} \mathbb{Z}_8$ since $\phi(8) = 4$. To see it's not cyclic, we need to write $(\mathbb{Z}_8)^\times$ down explicitly as follows

$$\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

It's clear all elements except identity has order 2, which implies $\operatorname{Aut} \mathbb{Z}_8$ is Klein four group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

For $n \geq 4$, it's left as an exercise for readers. □

Lemma 5.1.1. If G, H are two groups with relatively prime order p, q respectively, then any group homomorphism $\varphi : G \to H$ is trivial.

Proof. For arbitrary $x \in G$ with $o(x) = n$, we assume $o(\varphi(x)) = m$, then $n \mid p$ and $m \mid q$. Furthermore we have $m \mid n$, thus $m \mid p$, which implies $m \mid \gcd(p, q) = 1$, that is φ is trivial. □

Proposition 5.1.2. If G, H are two groups with relatively prime order, then $\operatorname{Aut}(G \times H) = \operatorname{Aut} G \times \operatorname{Aut} H$.

Proof. It's clear $\operatorname{Aut} G \times \operatorname{Aut} H \subseteq \operatorname{Aut}(G \times H)$: Given $\varphi_1 \in \operatorname{Aut} G, \varphi_2 \in \operatorname{Aut} H$, we can define an automorphism φ on $G \times H$ by

$$(g, h) \mapsto (\varphi_1(g), \varphi_2(h))$$

Note that inclusion in this direction puts no requirement on order of G, H.

Conversely, since order of G, H are relatively prime, then Lemma 5.1.1 implies $G \times \{e_H\}$ and $\{e_G\} \times H$ are characteristic subgroup of $G \times H$, that is subgroup which is invariant under automorphisms. Then restrict φ on these two subgroups to obtain $\varphi_1 \in \operatorname{Aut} G, \varphi_2 \in \operatorname{Aut} H$. □

Example 5.1.1. For $\mathbb{Z}_{12}$, we can write it as $\mathbb{Z}_3 \times \mathbb{Z}_4$, where 3 and 8 are relatively prime, thus

$$\begin{aligned}\operatorname{Aut}(\mathbb{Z}_{12}) &= \operatorname{Aut} \mathbb{Z}_3 \times \operatorname{Aut} \mathbb{Z}_4 \\ &= \mathbb{Z}_2 \times \mathbb{Z}_2\end{aligned}$$

Example 5.1.2. For $\mathbb{Z}_{24}$, we can write it as $\mathbb{Z}_3 \times \mathbb{Z}_8$, where 3 and 8 are relatively prime, thus

$$\begin{aligned}\operatorname{Aut}(\mathbb{Z}_{24}) &= \operatorname{Aut} \mathbb{Z}_3 \times \operatorname{Aut} \mathbb{Z}_8 \\ &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\end{aligned}$$

10 Given an abelian group G and if $x, y \in G$ are torsion element, then

1. Identity e is torsion, since $o(e) = 1$;
2. xy is torsion, since we must have $o(xy)$ divides $\operatorname{lcd}((o(x), o(y))$, which implies xy is finite;
3. x^{-1} is torsion, since $o(x^{-1}) = o(x)$.

We use T to denote subgroup consists of torsion element, then we claim G/T is torsion-free. Indeed, if $x+T$ is torsion in G/T, that is the smallest m such that $x^m \in T$ is finite, which implies there exists a finite n such that $(x^m)^n = e$, so x is torsion in G, that is $x \in T$.

6. Homework 6

6.1. **Sol for 2.11.**

1 Omit;
2 Omit;
3 Omit;
4 Omit;
5 It's clear that S_n is nilpotent when $n > 2$, since in this case center of S_n is trivial. To see S_3, S_4 are solvable, it suffices to show A_3, A_4 are solvable:
  (a) A_3 is clearly solvable, since $A_3 \cong \mathbb{Z}_3$;

  Remark 6.1.1. There is another way to show S_3 is solvable: Just note that $S_3 \cong D_3$, and we will show D_n is solvable in exercise 6.

  (b) Note that there exists a Klein four group K_4 in A_4 and it's normal. To see this, it suffices to write down all conjugacy classes of A_4 and check K_4 can be written as a union of conjugacy classes.
6 For a dihedral group $D_n = \{r, s \mid r^n = e, s^2 = e, srs^{-1} = r^{-1}\}$. It's clear cyclic subgroup generated by r is solvable and normal in D_n. Furthermore, the quotient $D_n/\langle r\rangle \cong \mathbb{Z}_2$ is also solvable. Thus D_n is solvable.
7 Omit;
8 Just consider $G = S_3$ and $K = A_3$.
9 Omit;
10 Let G be a group of order p^2q where p, q are distinct primes. To see G is solvable, it suffices to show either p-sylow subgroup or q-sylow subgroup is normal, since we already know a group with order p^2 or q is abelian.
  (a) If $p > q$, then p-sylow subgroup must be normal;
  (b) If $p < q$ and the number of q-sylow subgroups is p^2, then the number of elements with order q is $p^2(q-1)$. The remaining elements form only one p-sylow subgroup, which implies p-sylow subgroup is normal.

  Remark 6.1.2. In fact, there is the following theorem:

  Theorem 6.1.1 (Burnside theorem)**.** *If G is a finite group of order p^aq^b where p and q are distinct primes, and a and b are non-negative integers, then G is solvable.*

6.2. **Sol for 3.1.**

1 Omit;
2 Suppose R is a finite domain, then for any $0 \neq a \in R$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $a^n = e$, since R is finite. If $n = 1$, it's trivial; and if $n \geq 2$, then a^{n-1} is the inverse of a, which implies R is divisible.

  Remark 6.2.1. In fact, there is the following theorem:

  Theorem 6.2.1 (Wedderburn's little theorem)**.** *Every finite domain is a field.*

3 If there exists an idempotent $a \neq 0, 1$,

$$a(1-a) = 0$$

contradicts to the fact that the ring is a domain, since $a \neq 0, 1 - a \neq 0$.

Remark 6.2.2. In communicative algebra we're most interested in communicative ring with identity element, and they're closely related to geometry, which is called algebraic geometry. Here I want to show you some geometry explainations about idempotents. In the following of this remark, we always assume A is a communicative ring R with identity element e.

Definition 6.2.1 (spectrum of ring)**.** The set of all prime ideals in A is called the (prime) spectrum of A, denoted by $\operatorname{Spec} A$.

Bonus 6.2.1 (Zariski topology)**.** Given a subset E of A, $V(E)$ denotes all prime ideals of A which contain E. Prove that
1. If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a})$.
2. $V((0)) = X, V((1)) = \varnothing$.
3. if $(E_i)_{i\in I}$ is any family of subsets of A, then

$$V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$$

4. $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A.

These results show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski topology of $\operatorname{Spec} A$.

Bonus 6.2.2. Show that the following statements are equivalent:
(a) $X = \operatorname{Spec}(A)$ is disconnected.
(b) $A \cong A_1 \times A_2$ where neither of the rings A_1, A_2 is the zero ring.
(c) A contains an idempotent $\neq 0, 1$.
So as you can see, the geometry explaination of non-trivial idempotents is that they reprensent connected component of $\operatorname{Spec} A$ with respect to Zariski topology.

4 Omit;
8 Assume $\mathbb{Z}_n$ is generated by a, that is $a \in \mathbb{Z}_n$ is an element of order n, then a^m is a unit if and only if $(m, n) = 1$, so there are $\varphi(n)$ units in $\mathbb{Z}_n$, where φ is Euler function.
9 Omit;

Bonus 6.2.3. Let R be a ring, prove that:
(a) Any ideal of $M_n(R)$ takes the form $M_n(I)$, where I is an ideal of R.
(b) If R is a field, then $M_n(R)$ is a simple ring, that is a ring without non-trivial ideal.

10 Omit;

Remark 6.2.3. As Wedderburn's little theorem say, every finite domain is a field, in particular, every finite divisible ring is a field. So if you want to find a divisible ring which is not a field, you need to find them among infinite rings. An important example is exactly Hamilton quaternions $\mathbb{H}$. In fact, there is the following theorem:

Theorem 6.2.2 (Frobenius theorem)**.** All finite-dimensional[2] divisible rings containing a proper subring isomorphic to the real numbers are listed as follows:

1. Complex number $\mathbb{C}$;
2. Hamilton quaternions $\mathbb{H}$.

11 Omit;

[2]Here I mean the dimension as a $\mathbb{R}$-vector space.

7. Homework 7

7.1. **Sol for 3.2.**

1 Omit;
2 It's clear that $r(I)$ is an additive subgroup of R, and for all $r \in R, x \in r(I)$, we have
$$rxu = r0 = 0, \quad \forall u \in I$$
which implies $rs \in r(I)$.

Remark 7.1.1. Standard notation of $r(I)$ is $\operatorname{ann}(I)$, which is called annihilator of ideal[3] I.

3 It's clear that $(R : I)$ is an additive subgroup of R, since I is. and for all $r \in R, x \in (R : I)$, we have
$$r'(rx) \in U, \quad \forall r' \in R$$
which implies $rx \in (R : I)$.

Bonus 7.1.1. Show that[4]
$$(R : I) = \operatorname{ann}(R/I)$$

Remark 7.1.2. In general we can define
$$(\mathfrak{a} : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} \in \mathfrak{a}\}$$
where $\mathfrak{a}, \mathfrak{b}$ are two ideals of R.

Bonus 7.1.2. Show that
1. $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$
2. $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
3. $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$
4. $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$
5. $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$

where $\mathfrak{a}_i, \mathfrak{b}_i$ are ideals of R.

4 Omit;
5 Omit;
7 Omit;
8 Omit;
9 Omit;
11 Omit;
12 Omit;
13 Omit;

[3]I'm quite confused why textbook uses U to denote an ideal, standard notations for ideals are I, J or $\mathfrak{a}, \mathfrak{b}$.

[4]Almost trivial.

Remark 7.1.3. Local ring is a quite important object in communicative algebra or algebraic geometry. As what it's called, you can imagine a local ring reprensents a local piece of some geometric objects. Note that we said non-trivial idempotents reflect some disconnectness, and you can imagine a local piece of some geometric objects must be connected, and that's a view to understand the following one:

Bonus 7.1.3. A local ring contains no idempotents $\neq 0, 1$.

Later maybe I will show you an operation called localization, it's a technique to construct local rings. In $\operatorname{Spec} A$ we know that every point is a prime ideal, and localize A with respect to prime ideal $\mathfrak{p}$ is to focus on local properties of $\operatorname{Spec} A$ at point $\mathfrak{p}$.

16 Omit;

Remark 7.1.4. Firstly note that for a communicative ring A with identity, we have

Bonus 7.1.4. The nilradical of A is the intersection of all the prime ideals of A.

Thus every prime ideal of A contains our nilradical $\mathfrak{N}$, which implies as sets we have

$$\operatorname{Spec} A/\mathfrak{N} = V(\mathfrak{N}) = V((0)) = \operatorname{Spec} A$$

In fact you can prove

Bonus 7.1.5. $\operatorname{Spec} A$ is homeomorphic to $\operatorname{Spec} A/\mathfrak{N}$ with respect to Zariski topology.

So you may wonder what's the role of nilradical of A, in fact we have:

Bonus 7.1.6. A topological space X is said to be irreducible if $X \neq \varnothing$ and if every pair of non-empty open sets in X intersect, or equivalently if every non-empty open set is dense in X. Show that $\operatorname{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

Remark 7.1.5. To prove above, you may need to show the complement of $V(f), f \in A$, which is denoted by X_f, form a basis of Zariski topology, and note that:
1. $X_f \cap X_g = X_{fg}$;
2. $X_f = \varnothing$ if and only if f is nilpotent.

7.2. **Sol for 3.3.**

1 Omit;
2 Omit;
3 Since divisible ring R has no trivial ideal[5], so kernel of any endomorphism of R must be trivial, which implies it's injective.

[5]So do I.

Remark 7.2.1. In particular, any endomorphism of a field must be injective.

5 (a) Since any automorphism f maps 1 to 1, thus $f(n)$ is determined for all $n \in \mathbb{Z}$, and any element of $\mathbb{Q}$ can be written as mn^{-1}, which implies f is identity;
(b) Firstly we need to show for any automorphism f of $\mathbb{R}$, it's strictly increasing. Indeed, since for all $a \in \mathbb{R}^+$ we have $f(a) = f^2(\sqrt{a}) > 0$, which implies $f(a) - f(b) > 0$ if $a > b$. By the same argument you can show f is also identity on $\mathbb{Q}$, and for arbitrary irrational number r, you always can find two rational numbers a, b such that $a < r < b$ such that $a - b < \varepsilon$ for arbitrary small $\varepsilon > 0$. Then

$$a < f(r) < b$$

Take limit $\varepsilon \to 0$ to obtain $f(r) = r$.

6 Omit;
7 Omit;
12 Omit;

7.3. **Sol for 3.4.**

1 Omit;

Remark 7.3.1. In fact, it's localization with respect to S.

Bonus 7.3.1. If $S = A \backslash \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of a communicative ring A with identity, show A_S is a local ring.

Remark 7.3.2. Standard notation for localization with respect to prime ideal $\mathfrak{p}$ is $A_{\mathfrak{p}}$.

2 It's clear[6], since the fractional field of a domain R is exactly making all elements without 0 to be invertible.
3
4 Omit;
5 Omit;
6 Omit;
7 Omit;

Remark 7.3.3. In general, localization with respect to a multiplicative closed set S is also unique, since localization has some universal property, and any universal object is unique up to a unique isomorphism.

8 Omit;

[6]However, you need to check by definition.

8. Homework 8

8.1. **Sol for 3.5.**

1 Omit;
2 Omit;
3 Omit;
5 If $a+b\sqrt{-1}=(m+n\sqrt{-1})(d+e\sqrt{-1})$, then taking norm we have
$$p=a^2+b^2=(m^2+n^2)(d^2+e^2)$$
without lose of generality we may assume $m^2+n^2=1$, that is $m+n\sqrt{-1}$ is a unit in $\mathbb{Z}[\sqrt{-1}]$, which implies $a+bi$ is irreducible.
6
8 Omit;
9 If $p=ab$, where a,b are proper divisor of p, without lose of generality we may assume $p\mid a$, that is $a=pd$, thus
$$p=pdb$$
which implies $db=1$, since R is a domain, a contradiction to b is not unit.
10 Omit;

8.2. **Sol for 3.6.**

1 Omit;
3 Omit;
4 Omit;
5 Omit;
6 Let δ be a Euclidean valuation of a domain R, for all $a,b\in R, b\neq 0$, we write it as $a=bq+r$ with $r\neq 0$ and $\delta(r)<\delta(b)$. To see $\varphi=n+\delta$ is a Euclidean valuation, it suffices to see
(a) $n+\delta(r)<n+\delta(b)$;
(b) $n+\delta(a)\leq n+\delta(ab)$.
and it's trivial[7]. You can see $n\delta$ is also an Euclidean valuation by the same way.
7 Omit;
8 Omit;
9 Let $\alpha=a_1+a_2\sqrt{2}$ and $\beta=b_1+b_2\sqrt{2}$ be elements of $\mathbb{Z}[\sqrt{2}]$ with $\beta\neq 0$. We wish to show that there exist γ and δ in $\mathbb{Z}[\sqrt{2}]$ such that $\alpha=\gamma\beta+\delta$ and $N(\delta)<N(\beta)$. To that end, note that in $\mathbb{Q}(\sqrt{2})$ we have $\frac{\alpha}{\beta}=c_1+c_2\sqrt{2}$, where
$$c_1=\frac{a_1b_1-2a_2b_2}{b_1^2-2b_2^2},\quad c_2=\frac{a_2b_1-a_1b_2}{b_1^2-2b_2^2}$$
Let q_1 be an integer closest to c_1 and q_2 an integer closest to c_2; then $|c_1-q_1|\leqslant 1/2$ and $|c_2-q_2|\leqslant 1/2$. Now let $\gamma=q_1+q_2\sqrt{2}$; certainly $\gamma\in\mathbb{Z}[\sqrt{2}]$. Next, let $\theta=(c_1-q_1)+(c_2-q_2)\sqrt{2}$. We have $\theta=\frac{\alpha}{\beta}-\gamma$, so

[7] A quite boring problem.

that $\theta\beta = \alpha - \gamma\beta$ Letting $\delta = \theta\beta$, we have $\alpha = \gamma\beta + \delta$. It remains to be shown that $N(\delta) < N(\beta)$. To that end, note that

$$N(\theta) = |(c_1 - q_1)^2 - 2(c_2 - q_2)^2| \leqslant |(c_1 - q_1)^2| + | - 2(c_2 - q_2)^2|$$

by the triangle inequality. Thus we have

$$N(\theta) \leqslant (c_1 - q_1)^2 + 2(c_2 - q_2)^2 \leqslant (1/2)^2 + 2(1/2)^2 = 3/4.$$

In particular, $N(\delta) \leqslant \frac{3}{4}N(\beta)$ as desired.

10 Omit;

References

Yau Mathematical Sciences Center, Tsinghua University, Beijing, 100084, P.R. China,
Email address: `liubw22@mails.tsinghua.edu.cn`