

## MATH 113 HOMEWORK 5 SOLUTIONS

### 1. THE ISOMORPHISM THEOREMS

**Problem 1.1.** Let  $C \leq \mathbb{C}^*$  be the circle group. Use the first isomorphism theorem to show that:

- (1)  $\mathbb{R}/\mathbb{Z} \cong C$ .
- (2) There is a subgroup of  $C$  which is isomorphic to  $\mathbb{Q}/\mathbb{Z}$ .
- (3)  $\mathbb{C}^*/C \cong (\mathbb{R}_{>0}, \cdot)$ , the group of positive real numbers with multiplication.

**Solution 1.1.1** (Part 1). Define a homomorphism  $\phi : \mathbb{R} \rightarrow C$  by  $\phi(\theta) = \text{cis}(2\pi\theta)$ . It is easy to check that  $\phi$  is indeed a homomorphism. The map  $\phi$  is surjective since every element of  $C$  is of the form  $\text{cis}(\alpha) = \text{cis}(2\pi \frac{\alpha}{2\pi}) = \phi(\frac{\alpha}{2\pi})$  for some  $\alpha \in \mathbb{R}$ . The kernel of  $\phi$  is the set of  $\theta \in \mathbb{R}$  such that  $\text{cis}(2\pi\theta) = 1$ ; this equation holds true if and only if  $2\pi\theta = 2\pi k$  for some  $k \in \mathbb{Z}$ . Dividing by  $2\pi$  we see that  $\ker(\phi) = \mathbb{Z}$ , so the first isomorphism theorem tells us that  $\mathbb{R}/\mathbb{Z} \cong C$ .

**Solution 1.1.2** (Part 2). Since  $\mathbb{Q}/\mathbb{Z}$  is a subgroup of  $\mathbb{R}/\mathbb{Z}$  and  $\mathbb{R}/\mathbb{Z} \cong C$ , this follows immediately from part (1). Working carefully through part (1), we see that in terms of  $C$ , this subgroup corresponds to all points in  $C$  which have angles which are *rational* multiples of  $2\pi$ . This is precisely the torsion subgroup of  $C$ .

**Solution 1.1.3** (Part 3). Define a homomorphism  $\phi : \mathbb{C}^* \rightarrow \mathbb{R}_{>0}$  by  $\phi(z) = |z|$ . Since  $|zw| = |z||w|$ , this is in fact a homomorphism. It is surjective since if  $a$  is a positive real number, then  $a$  is also a complex number, and  $a = |a|$ . The kernel of  $\phi$  is the set of  $z \in \mathbb{C}^*$  such that  $|z| = 1$ ; by definition this is  $C$ , so the first isomorphism theorem tells us that  $\mathbb{C}^*/C \cong \mathbb{R}_{>0}$ .

**Problem 1.2** (The Universal Property of the Quotient). Let  $G$  be a group and let  $N$  be a normal subgroup of  $G$ . Let  $\phi : G \rightarrow G/N$  be the canonical homomorphism.

- (1) Let  $H$  be another group and let  $f : G \rightarrow H$  be a homomorphism. Show that there is a homomorphism  $\bar{f} : G/N \rightarrow H$  such that  $\bar{f} \circ \phi = f$  if and only if  $N \leq \ker(f)$ . Moreover, show that  $\bar{f}$  is unique if it exists.
- (2) Use (1) to show that there is a surjective homomorphism  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  if and only if  $m|n$ .

**Solution 1.2.1** (Part 1). Let  $g \in G$  be arbitrary. The equation  $f = \bar{f} \circ \phi$  says that  $f(g) = \bar{f}(\phi(g)) = \bar{f}(gN)$ , so this equation forces the definition of  $\bar{f}$  on us, so uniqueness is immediate (another way of saying this:  $\phi$  is

surjective).

Now, we want to show that the function  $\bar{f}$  defined by  $\bar{f}(gN) = f(g)$  is well-defined if and only if  $N \leq \ker(f)$ . Suppose first that  $N \leq \ker(f)$ , and that  $g_1N = g_2N$ . Then  $g_2^{-1}g_1 \in N \leq \ker(f)$ , so  $f(g_2^{-1}g_1) = e$ . Expanding this out we get  $e = f(g_2)^{-1}f(g_1)$ , so  $f(g_2) = f(g_1)$ , i.e.  $\bar{f}(g_2N) = \bar{f}(g_1N)$ . Hence  $\bar{f}$  is well-defined.

Suppose on the other hand that  $\bar{f}$  is well-defined, and let  $n \in N$  be arbitrary. Then  $eN = nN$ , so

$$e_H = f(e_G) = \bar{f}(eN) = \bar{f}(nN) = f(n),$$

so  $n \in \ker(f)$ , i.e.  $N \leq \ker(f)$ .

Finally, note that  $\bar{f}$  is indeed a homomorphism when defined; we have

$$\bar{f}(g_1Ng_2N) = \bar{f}(g_1g_2N) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1N)\bar{f}(g_2N).$$

**Solution 1.2.2** (Part 2). By part (1), to give a surjective homomorphism  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  is the same as giving a surjective homomorphism  $g : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  such that  $n\mathbb{Z} \leq \ker(g)$ . Now, to give such a homomorphism  $g$ , it is enough to specify  $g(1)$ ; suppose  $g(1) = a$ . Then for all  $k \in \mathbb{N}$  we have  $g(k) = g(1 + \cdots + 1) = g(1) + \cdots + g(1) = ka$ , and  $g(-k) = -g(k) = -ka$ , so  $g$  is totally determined by  $g(1)$ .

On the other hand, for every  $a \in \mathbb{Z}/m\mathbb{Z}$ , the function  $g : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  defined by  $g(k) = ka$  is a homomorphism, as we have already seen in class. So, the question becomes: for which  $a$  is the corresponding homomorphism  $g$  surjective, and for which  $a$  is  $n\mathbb{Z} \leq \ker(g)$ ?

We already know the answer to the first question:  $g$  is surjective if and only if  $a$  is a generator for  $\mathbb{Z}/m\mathbb{Z}$  (by definition!), and this happens if and only if  $\gcd(m, a) = 1$ . On the other hand,  $n\mathbb{Z} \leq \ker(g)$  if and only if  $g(n) = 0$ , i.e. if and only if  $na = 0$ . This happens if and only if  $o(a)|n$ .

We conclude that there is a surjective homomorphism from  $\mathbb{Z}/n\mathbb{Z}$  to  $\mathbb{Z}/m\mathbb{Z}$  if and only if there is a generator  $a$  of  $\mathbb{Z}/m\mathbb{Z}$  such that  $o(a)|n$ . But  $o(a) = m$ , so such a generator exists if and only if  $m|n$ .

**Problem 1.3.** Let  $G$  be a group, let  $N \triangleleft G$  be a normal subgroup, and let  $K \leq G$  be another subgroup. Let  $\phi : G \rightarrow G/N$  be the canonical homomorphism. Show that  $\phi(K) = KN/N$  (i.e. show that  $\phi(K)$  and  $KN/N$  are the same subgroup of  $G/N$ , not just isomorphic).

**Solution 1.3.1.** We have  $KN = \{kn \mid k \in K, n \in N\}$ , so  $KN/N = \{knN \mid k \in K, n \in N\}$ . We have  $knN = kN$  for all  $k \in K, n \in N$ , so  $KN/N = \{kN \mid k \in K\} = \phi(K)$ .

**Problem 1.4.** Do Judson, Ch. 9, Exercise 11:

In the group  $\mathbb{Z}/24\mathbb{Z}$ , let  $H = \langle 4 \rangle$ ,  $N = \langle 6 \rangle$ .

- (1) List the elements of  $H + N$  and  $H \cap N$ .
- (2) List the cosets in  $H + N/N$ .
- (3) List the cosets in  $H/H \cap N$ .
- (4) Describe the correspondence of the second iso theorem in this case.

**Solution 1.4.1.** (1)  $H + N = \{4a + 6b \mid a, b \in \mathbb{Z}\} = \langle 2 \rangle$ ,  $H \cap N = \langle 12 \rangle$ .  
 (2) The elements of  $H+N/N$  are  $0+N = \{0, 6, 12, 18\}$ ,  $2+N = \{2, 8, 14, 20\}$ ,  
 and  $4+N = \{4, 10, 16, 22\}$ .  
 (3) The elements of  $H/H \cap N$  are  $0+H \cap N = \{0, 12\}$ ,  $4+H \cap N = \{4, 16\}$ ,  
 and  $8+H \cap N = \{8, 20\}$ .  
 (4) The isomorphism  $H/H \cap N \rightarrow H+N/N$  is given by  $h+H \cap N \mapsto h+N$ .  
 So in this case the iso takes  $0+H \cap N \mapsto 0+N$ ,  $4+H \cap N \mapsto 4+N$ , and  
 $8+H \cap N \mapsto 8+N = 2+N$ .

**Problem 1.5.** Consider the group  $D_6$ , and let  $H = \langle r^2 \rangle$  and  $K = \langle r^3 \rangle$  in  $D_6$ . Show that  $H$  and  $K$  are both normal subgroups of  $D_6$ . Calculate  $D_6/H$  and  $D_6/K$ , and use this calculation to compute the subgroup lattice of  $D_6$ .

**Solution 1.5.1.** Since every element of  $D_6$  is of the form  $r^k s^\ell$ , to show that  $H$  and  $K$  are normal it suffices to show that  $rHr^{-1} = H$  and  $sHs^{-1} = H$ , and likewise for  $K$ . It is obvious that  $rHr^{-1} = H$  and  $rKr^{-1} = K$  since  $r$  commutes with all of the elements in  $H$  and  $K$ . We have  $sHs^{-1} = \{ses^{-1}, sr^2s^{-1}, sr^4s^{-1}\} = \{e, r^4, r^2\} = H$ , and  $sKs^{-1} = \{ses^{-1}, sr^3s^{-1}\} = \{e, r^3\} = K$ , so  $H$  and  $K$  are normal.

Let us first consider  $D_6/H$ . This is a group of order  $\frac{12}{3} = 4$ , so is either cyclic or isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . The four elements of this group are

$$\begin{aligned} H &= r^2H = r^4H, & rH &= r^3H = r^5H \\ sH &= r^2sH = r^4sH, & rsH &= r^3sH = r^5sH. \end{aligned}$$

It is easy to check that all of these elements have order 2, so  $D_6/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Hence the subgroups of  $D_6/H$  are given by the whole group, the trivial subgroup, and the subgroups  $\langle rH \rangle$ ,  $\langle sH \rangle$ , and  $\langle rsH \rangle$ . Let  $\phi : D_6 \rightarrow D_6/H$  be the canonical homomorphism. Taking preimages, we find that the subgroups of  $D_6$  which contain  $H$  (i.e. which contain  $r^2$ ) are

$$\begin{aligned} \phi^{-1}(\langle rH \rangle) &= \langle r \rangle, \\ \phi^{-1}(\langle sH \rangle) &= \{e, r^2, r^4, s, r^2s, r^4s\} =: \langle r^2, s \rangle, \text{ and} \\ \phi^{-1}(\langle rsH \rangle) &= \{e, r^2, r^4, rs, r^3s, r^5s\} =: \langle r^2, rs \rangle. \end{aligned}$$

Now let us consider  $D_6/K$ . This is a group of order  $\frac{12}{2} = 6$ , so there are more possibilities. The elements of  $D_6/K$  are

$$\begin{aligned} K &= r^3K, & rK &= r^4K, & r^2K &= r^5K, \\ sK &= r^3sK & rsK &= r^4sK & r^2sK &= r^5sK. \end{aligned}$$

This group is isomorphic to  $S_3$ . There are several ways to see this, but we don't actually need to prove this; it's enough to notice that since this is a group of order 6, the only subgroups must be cyclic subgroups and the whole group (by Lagrange's Theorem, this is true for any group of order  $pq$  with  $p$  and  $q$  different primes). So the nontrivial subgroups are

$$\begin{aligned} \langle rK \rangle &= \{K, rK, r^2K\}, \langle sK \rangle = \{K, sK\}, \\ \langle rsK \rangle &= \{K, rsK\}, \text{ and } \langle r^2sK \rangle = \{K, r^2sK\}. \end{aligned}$$

Let  $\psi : D_6 \rightarrow D_6/K$  be the canonical homomorphism. Again by the lattice isomorphism theorem, the subgroups of  $D_6$  which contain  $K$  (i.e. which contain  $r^3$ ) are precisely

$$\begin{aligned}\psi^{-1}(\langle rK \rangle) &= \langle r \rangle, \\ \psi^{-1}(\langle sK \rangle) &= \{e, r^3, s, r^3s\} =: \langle r^3, s \rangle, \\ \psi^{-1}(\langle rsK \rangle) &= \{e, r^3, rs, r^4s\} =: \langle r^3, rs \rangle, \text{ and} \\ \psi^{-1}(\langle r^2sK \rangle) &= \{e, r^3, r^2s, r^5s\} =: \langle r^3, r^2s \rangle.\end{aligned}$$

So, we now know all of the subgroups of  $D_6$  which contain a power of  $r$ . So, it remains to see what subgroups contain *no* power of  $r$ , i.e. which subgroups are a subset of  $\{e, s, rs, r^2s, r^3s, r^4s, r^5s\}$ . It is easy to see that any two non-identity elements of this set multiply together to give a nontrivial power of  $r$  (for example  $r^2sr^3s = r^5$ ), so the only such subgroups must be the cyclic subgroups generated by each of these elements. A quick check shows that all of these elements (besides  $e$ ) have order 2, so the remaining subgroups of  $D_6$  are

$$\{e\}, \langle s \rangle, \langle rs \rangle, \langle r^2s \rangle, \langle r^3s \rangle, \langle r^4s \rangle, \text{ and } \langle r^5s \rangle.$$

I leave it to you to put this information together into a lattice.

## 2. THE STRUCTURE THEOREM FOR FINITELY GENERATED ABELIAN GROUPS

**Problem 2.1.** Do the following:

- (1) List all abelian groups of order 24.
- (2) List all abelian groups of order 81.
- (3) Show that every abelian group of order 30 is cyclic.

**Solution 2.1.1.** (1) We have  $24 = 2^3 \cdot 3$ , so the abelian groups of order 24 are

$$\begin{aligned}\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/24\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \text{ and} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.\end{aligned}$$

- (2) We have  $81 = 3^4$ , so the abelian groups of order 81 are

$$\begin{aligned}\mathbb{Z}/81\mathbb{Z}, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}, \\ \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \text{ and} \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.\end{aligned}$$

- (3) Since  $30 = 2 \cdot 3 \cdot 5$  has no repeated primes in its factorization, the only abelian group of order 30 is

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}.$$

**Problem 2.2** (Invariant Factors). Suppose that  $A$  is an abelian group of the form

$$A = \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z},$$

where  $a_1|a_2|\cdots|a_n$ . We know that  $A$  can be written uniquely as a product

$$A \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

Do the following:

- (1) Explain how to recover the numbers  $a_1, \dots, a_n$  from  $p_1^{e_1}, \dots, p_k^{e_k}$ .
- (2) Elaborating on (1), explain how every finite abelian group can be written uniquely as

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

for some  $a_1, \dots, a_n \in \mathbb{N}$  with  $a_1|a_2|\cdots|a_n$ .

- (3) Carry out the process you described in (2) for the group

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

**Solution 2.2.1** (Part 1). Let  $q_1, \dots, q_k$  be the primes appearing in the prime factorizations of  $a_1, \dots, a_n$ . Since  $a_1|a_2|\cdots|a_n$ , all of these primes appear in the prime factorization of  $a_n$ , and for each  $a_i$ , the power of  $q_j$  which divides  $a_i$  is less than or equal to the power of  $q_j$  which divides  $a_n$ . So, from the list  $p_1^{e_1}, \dots, p_k^{e_k}$ , we can find the prime factors of  $a_n$  by looking for the *largest* power of each distinct prime  $p$  which appears. Removing these factors, we can find the prime factors of  $a_{n-1}$  by looking for the largest remaining power of each prime  $p$ , and so on. Hence the  $a_i$  are uniquely determined by the  $p_j^{e_j}$ .

**Solution 2.2.2** (Part 2). Part (1) already shows uniqueness, so it remains to show that every finite abelian group can be written in this form. But we have already described an algorithm for doing this: if

$$A \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$$

is any finite abelian group, then let  $a_n$  be the product of the largest power of  $p$  which appears in this expression for each prime  $p$ , let  $a_{n-1}$  be the product of the largest remaining powers, and so on. Then

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

is the desired expression; the fact that  $A$  is isomorphic to this group follows from the fact that  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}/q_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell^{k_\ell}\mathbb{Z}$  where  $n = q_1^{k_1} \cdots q_\ell^{k_\ell}$  is the prime factorization of  $n$ , and the fact that  $a_i|a_{i+1}$  for each  $i$  follows directly from the construction of the  $a_i$ .

**Solution 2.2.3** (Part 3). The largest power of 2 appearing is 4, the largest power of 3 is 9, and the largest power of 7 is 7, so let  $a_n = 4 \cdot 9 \cdot 7 = 252$ . The largest power of 2 that remains is 4, the largest power of 3 that remains is 3, and the largest power of 7 that remains is 7, so let  $a_{n-1} = 4 \cdot 3 \cdot 7 = 84$ .

The only remaining factor is a 2, so  $a_{n-2} = 2$ . This is our last factor, so  $n = 3$  and the desired expression is

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z}.$$

**Problem 2.3.** Let  $A$  be an abelian group. Show that  $\text{rank}(A) = \text{rank}(A/T(A))$ , where  $T(A)$  is the torsion subgroup of  $A$ .

**Solution 2.3.1.** The canonical homomorphism  $\phi : A \rightarrow A/T(A)$  is surjective, so  $\text{rank}(A/T(A)) \leq \text{rank}(A)$ . It remains to show that  $\text{rank}(A) \leq \text{rank}(A/T(A))$ . Suppose that  $a_1, \dots, a_n$  are linearly independent elements of  $A$ . I claim that they are also linearly independent in  $A/T(A)$ . Suppose that

$m_1(a_1 + T(A)) + \dots + m_n(a_n + T(A)) = m_1a_1 + \dots + m_na_n + T(A) = 0 + T(A)$  in  $A/T(A)$ , for some  $m_1, \dots, m_n \in \mathbb{Z}$ . Then  $m_1a_1 + \dots + m_na_n \in T(A)$ , so there is some positive  $k \in \mathbb{N}$  such that

$$km_1a_1 + \dots + km_na_n = 0.$$

Now, since  $a_1, \dots, a_n$  are linearly independent in  $A$ , it follows that  $km_1 = km_2 = \dots = km_n = 0$ . But  $k \neq 0$ , so  $m_1 = \dots = m_n = 0$ , hence the elements  $a_1 + T(A), \dots, a_n + T(A)$  are linearly independent in  $A/T(A)$ . Thus  $\text{rank}(A) \leq \text{rank}(A/T(A))$ , as desired.