

MATH 113 HOMEWORK 4 SOLUTIONS

1. BASIC PROBLEMS

Problem 1.1. Show that every group of order 4 is isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution 1.1.1. Let G be a group of order 4. Then every element $g \in G$ has order dividing 4, hence has order 1, 2, or 4. If G has an element of order 4, then G is cyclic, so $G \cong \mathbb{Z}/4\mathbb{Z}$. So, assume that G is not cyclic; then every non-identity element of G has order 2. Write $G = \{e, a, b, c\}$ where e is the identity element of G and a, b, c are the remaining elements. By our assumption, $a^2 = b^2 = c^2 = e$. By Homework 2, Problem 6, it follows that G is abelian.

Now, let us work out what ab is, for example. We know that either:

- (1) $ab = e$,
- (2) $ab = a$,
- (3) $ab = b$, or
- (4) $ab = c$.

In case (1), we have $b = a^{-1} = a$, a contradiction. In case (2), multiplying on the left by a^{-1} gives $b = e$, a contradiction, and similarly (3) yields $a = e$, a contradiction. Thus $ab = c$. Exactly the same reasoning shows that $ac = b$ and $bc = a$ (Note: this also shows $ba = c$, etc, so we could prove that G is abelian this way as well).

So, now, define a function

$$\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow G$$

by $\phi(0, 0) = e$, $\phi(1, 0) = a$, $\phi(0, 1) = b$, and $\phi(1, 1) = c$. I claim that ϕ is an isomorphism. It is clearly a bijection. For any element $x \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have

$$\phi(x + (0, 0)) = \phi(x) = \phi(x) \cdot e = \phi(x)\phi(0, 0),$$

and by hand we check:

$$\begin{aligned} \phi((1, 0) + (1, 0)) &= \phi(0, 0) = e = a^2 = \phi(1, 0)\phi(1, 0) \\ \phi((1, 0) + (0, 1)) &= \phi(1, 1) = c = ab = \phi(1, 0)\phi(0, 1) \\ \phi((1, 0) + (1, 1)) &= \phi(0, 1) = b = ac = \phi(1, 0)\phi(1, 1) \\ \phi((0, 1) + (0, 1)) &= \phi(0, 0) = e = b^2 = \phi(0, 1)\phi(0, 1) \\ \phi((0, 1) + (1, 1)) &= \phi(1, 0) = a = bc = \phi(0, 1)\phi(1, 1) \\ \phi((1, 1) + (1, 1)) &= \phi(0, 0) = e = c^2 = \phi(1, 1)\phi(1, 1). \end{aligned}$$

Hence ϕ is an isomorphism, so $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 1.2. Use Fermat's Little Theorem to show that if $p \in \mathbb{N}$ is prime and $p \equiv 3 \pmod{4}$ then there is no solution to the equation

$$x^2 \equiv -1 \pmod{p}.$$

Give an example that shows that this equation *can* have solutions if $p \equiv 1 \pmod{4}$.

Solution 1.2.1. Suppose that $p \equiv 3 \pmod{4}$. Then $p = 3 + 4n$ for some $n \in \mathbb{Z}$, so $p - 1 = 2 + 4n$ for some $n \in \mathbb{Z}$. Let $x \in \mathbb{Z}$ be arbitrary. If $p|x$, then $x \equiv 0 \pmod{p}$, then $x^2 \equiv 0 \pmod{p}$ also, so x is not a solution to our equation. On the other hand, suppose $p \nmid x$. Then $\gcd(p, x) = 1$, and by Fermat's little theorem, we have

$$x^{p-1} \equiv x^{2+4n} \equiv 1 \pmod{p}.$$

Now, suppose that

$$x^2 \equiv -1 \pmod{p}.$$

Then $x^4 \equiv (-1)^2 \equiv 1 \pmod{p}$, so

$$1 \equiv x^{2+4n} \equiv x^2(x^4)^n \equiv x^2 \pmod{p}.$$

Thus

$$1 \equiv x^2 \equiv -1 \pmod{p},$$

i.e. p divides $1 - (-1) = 2$. Thus $p = 2$, contradicting our assumption that $p \equiv 3 \pmod{4}$. Hence no solution to the equation exists.

On the other hand, notice that

$$2^2 \equiv 4 \equiv -1 \pmod{5},$$

so this equation can have solutions when $p \equiv 1 \pmod{4}$.

Problem 1.3. Let G be a group. Recall that an *automorphism* of G is an isomorphism $f : G \rightarrow G$.

- (1) Show that the set of automorphisms of G forms a group; we denote this group $\text{Aut}(G)$.
- (2) Show that $\text{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.
- (3) Calculate $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, and show that this group is isomorphic to a group we are already very familiar with.

Solution 1.3.1 (Solution to (1)). We can consider $\text{Aut}(G)$ as a subset of S_G , the group of permutations of the elements of G . It suffices to show that $\text{Aut}(G)$ is a subgroup of S_G . We know already that the identity function is an automorphism of G and that if ϕ is an automorphism of G then ϕ^{-1} is also. So, it suffices to show that if ϕ and ψ are automorphisms of G , then $\phi \circ \psi$ is also. Since ϕ and ψ are bijections, so is $\phi \circ \psi$. We need only to show that $\phi \circ \psi$ is still a homomorphism. Let $g, h \in G$ be arbitrary. We have

$$(\phi \circ \psi)(gh) = \phi(\psi(gh)) = \phi(\psi(g)\psi(h)) = \phi(\psi(g))\phi(\psi(h)) = (\phi \circ \psi)(g)(\phi \circ \psi)(h).$$

This $\phi \circ \psi$ is a homomorphism, and we are done.

Solution 1.3.2 (Solution to (2)). Let $\phi : \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ be an automorphism. The function ϕ is totally determined by $\phi(1)$, since

$$\phi(n) = \phi(1 + 1 + \cdots + 1) = \phi(1) + \phi(1) + \cdots + \phi(1) = n \cdot \phi(1),$$

as ϕ is a homomorphism. Since ϕ is an isomorphism and 1 has order 4 in $\mathbb{Z}/4\mathbb{Z}$, $\phi(1)$ must also have order 4, hence $\phi(1) = 1$ or 3. Thus there are at most two automorphisms of $\mathbb{Z}/4\mathbb{Z}$. One of these automorphisms is the identity function, so to show that $\text{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, it suffices to show that there is a non-identity automorphism of $\mathbb{Z}/4\mathbb{Z}$.

Define $\phi : \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ by $\phi(n) = 3n$. Then ϕ is well-defined: if $n = n'$ in $\mathbb{Z}/4\mathbb{Z}$ then $4|(n - n')$, so $4|(3n - 3n')$, hence $3n = 3n'$ in $\mathbb{Z}/4\mathbb{Z}$. And ϕ is a homomorphism since $\phi(n + n') = 3(n + n') = 3n + 3n'$. It is easy to see that ϕ is surjective, hence injective, so ϕ is an automorphism. And ϕ is not the identity function since $\phi(1) = 3 \neq 1$.

Solution 1.3.3 (Solution to (3)). By inspection, it appears that we can use an automorphism to permute the non-identity elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in any way we choose. Since there are three non-identity elements of this group, this suggests that $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. We will show that this is the case; the argument is sort of formal, but keeping the above in mind should make it easier to follow.

Let $a = (1, 0)$, $b = (0, 1)$ and $c = (1, 1)$ be the non-identity elements of $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and write 0 for the identity. We have that

$$2a = 2b = 2c = 0 \quad \text{and} \quad a + b = c, a + c = b, b + c = a,$$

i.e. adding any element to itself in this group gives 0, whereas adding two different non-identity elements always yields the third non-identity element. Let σ be any permutation of the set $\{a, b, c\}$. I claim that the function $f_\sigma : G \rightarrow G$ given by $f_\sigma(0) = 0$ and $f_\sigma(x) = \sigma(x)$ for $x \neq 0$ is an automorphism. Indeed, we have $f_\sigma(0 + x) = f_\sigma(x) = f_\sigma(0) + f_\sigma(x)$, and we have:

$$\begin{aligned} f_\sigma(a + a) &= f_\sigma(0) = 0 = f_\sigma(a) + f_\sigma(a) \\ f_\sigma(b + b) &= f_\sigma(0) = 0 = f_\sigma(b) + f_\sigma(b) \\ f_\sigma(c + c) &= f_\sigma(0) = 0 = f_\sigma(c) + f_\sigma(c). \end{aligned}$$

So it remains to check $f_\sigma(a + b)$, $f_\sigma(a + c)$, $f_\sigma(b + c)$. For example, we have $f_\sigma(a + b) = f_\sigma(c) = \sigma(c)$, which is some non-identity element of G . Since σ is a bijection from $\{a, b, c\}$ to itself, $\sigma(a)$ and $\sigma(b)$ are the remaining non-identity elements of G , and hence $\sigma(a) + \sigma(b) = \sigma(c)$, i.e.

$$f_\sigma(a) + f_\sigma(b) = \sigma(a) + \sigma(b) = \sigma(c) = f_\sigma(c) = f_\sigma(a + b),$$

and similarly for the other pairs. Thus f_σ is an automorphism of G . Now, since an automorphism of G must send 0 to 0 and permute the remaining elements, the f_σ are all possible automorphisms of G . Now, let σ, τ be two permutations of $\{a, b, c\}$. Then for $x \in \{a, b, c\}$, we have

$$f_\sigma f_\tau(x) = f_\sigma(\tau(x)) = \sigma\tau(x) = f_{\sigma\tau}(x),$$

and $f_\sigma f_\tau(0) = 0$ clearly, hence $f_\sigma f_\tau = f_{\sigma\tau}$. Define a function

$$f : S_3 \rightarrow \text{Aut}(G)$$

by $f(\sigma) = f_\sigma$ (considering S_3 as the permutations of $\{a, b, c\}$). The above shows that f is a homomorphism and that f is surjective. It remains to show that f is injective, but this is also clear: if $f_\sigma = f_\tau$, then for all $x \in \{a, b, c\}$, we have

$$\sigma(x) = f_\sigma(x) = f_\tau(x) = \tau(x),$$

hence $\sigma = \tau$. Thus f is an isomorphism.

2. BASIC PROBLEMS PART 2

Problem 2.1. Do Judson, Ch. 9, Exercise 6.

Solution 2.1.1. Parts (a) and (b) are straightforward. To prove normality, we calculate:

$$\begin{aligned} & \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} \\ = & \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix} \begin{pmatrix} c/ac & -b/ac \\ 0 & a/ac \end{pmatrix} = \begin{pmatrix} 1 & -ab/ac + (a^2x+ab)/ac \\ 0 & 1 \end{pmatrix} \in U. \end{aligned}$$

The nicest way to prove (d) is using the first isomorphism theorem: define a homomorphism $\phi : T \rightarrow (\mathbb{R}^*)^2$ by

$$\phi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c).$$

Then we check that ϕ is actually a homomorphism:

$$\begin{aligned} \phi \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) &= \phi \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \\ &= (aa', cc') \\ &= (a, c)(a', c') \\ &= \phi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \phi \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \end{aligned}$$

It is easy to see that ϕ is surjective, and that $\ker(\phi) = U$. Hence $T/U \cong (\mathbb{R}^*)^2$, so T/U is in particular abelian.

Problem 2.2. Let G be a group and let H be a normal subgroup of G such that $[G : H]$ is finite. Suppose there is some element $g \in G$ such that $g \notin H$ but $g^2 \in H$. Show that $[G : H]$ is even.

Solution 2.2.1. Consider the element $gH \in G/H$. Since $g \notin H$, we have $gH \neq H$, so gH is not the identity element of G/H . But $(gH)^2 = g^2H = H$ since $g^2 \in H$. Hence gH has order 2 in G/H . Since the order of an element divides the order of the group, 2 divides $|G/H| = [G : H]$, hence $[G : H]$ is even.

Problem 2.3. Let G be a group and let H be a subgroup of G . Show that H is normal in G if and only if the set of left cosets of H is equal to the set of right cosets of H , i.e.

$$\{gH \mid g \in G\} = \{Hg \mid g \in G\}.$$

Use this to give a second proof that if $[G : H] = 2$ then H is normal.

Solution 2.3.1. Clearly if H is normal then the set of left cosets of H is equal to the set of right cosets of H .

Suppose on the other hand that

$$\{gH \mid g \in G\} = \{Hg \mid g \in G\}.$$

Let $g \in G$ be arbitrary; we want to show that $gH = Hg$. We know that $gH = Hg'$ for some $g' \in G$ by assumption. Hence

$$g = ge \in gH = Hg',$$

so $g \in Hg'$, i.e. $g = hg'$ for some $h \in H$. I claim that this implies that $Hg = Hg'$. Indeed, let $h' \in H$ be arbitrary. Then $h'g = (h'h)g \in Hg'$, so $Hg \subseteq Hg'$. On the other hand, $h'g' = h'h^{-1}hg' = (h'h^{-1})g \in Hg$, so $Hg' \subseteq Hg$. Hence we have

$$gH = Hg' = Hg,$$

as desired.

So, suppose that $[G : H] = 2$. Then the left cosets of H in G must be H and $G \setminus H$, since the left cosets of H form a partition of G and there are only two left cosets. Likewise, the right cosets of H in G must be H and $G \setminus H$ for the same reason. Thus the set of left cosets of H is the same as the set of right cosets of H , so H is normal in G .

Problem 2.4. Let G be a group. Recall that the *center* $Z(G)$ of G is defined by

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

- (1) Show that $Z(G)$ is a normal subgroup of G .
- (2) Calculate $Z(D_4)$.

Solution 2.4.1 (Solution to (1)). Let $a \in Z(G)$ and $g \in G$ be arbitrary. We have to show that $gag^{-1} \in Z(G)$. But $gag^{-1} = gg^{-1}a = a \in Z(G)$ since a commutes with all elements of G . Hence $Z(G)$ is normal.

Solution 2.4.2. I claim that $Z(D_4) = \{e, r^2\}$. Clearly $e \in Z(G)$; as for r^2 , it is enough to show that r^2 commutes with r and s since every element of D_4 is a product of the elements r and s . We have $rr^2 = r^3 = r^2r$ and $sr^2 = r^{-2}s = r^2s$, as desired.

It remains to show that this is the whole center of D_4 , i.e. for every other element $a \in D_4$ we need to exhibit an element $b \in D_4$ which does not commute with a . We have

$$sr = r^{-1}s = r^3s \neq rs,$$

so $r, s \notin Z(D_4)$. Likewise, we have $(r^3)(rs) = r^4s = s$, but

$$(rs)(r^3) = rr^{-3}s = r^2s \neq s,$$

so also $r^3, rs \notin Z(D_4)$. Similarly,

$$(r^2s)r = rs \neq r^3s = r(r^2s),$$

so $r^2s \notin Z(D_4)$. Finally,

$$(r^3s)s = r^3 \neq r = s(r^3s),$$

so $r^3s \notin Z(D_4)$.