Math 120 HW1 Solutions

Xiaoyu He, edits by Prof. Church

April 8, 2018

Exercise 1.1.8a

Let $G = \{z \in \mathbb{C} | z^n = 1$ for some $n \in \mathbb{Z}^+\}$. Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

There are four things to check:

1. G is closed under multiplication. If $z_1, z_2 \in G$, then there exist $n_1, n_2 \in \mathbb{Z}^+$ for which $z_1^{n_1} = z_2^{n_2} = 1$. Set $z = z_1 z_2$ and $n = n_1 n_2$. Then, because multiplication in $\mathbb{C}$ commutes,
$$z^n = (z_1 z_2)^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{n_1} = 1^{n_2} \cdot 1^{n_1} = 1.$$
Thus, $z_1 z_2 \in G$ as well.
2. G contains an identity. The identity is the complex number 1, which lies in G because $1^1 = 1$. Because $1 \cdot z = z$ for any $z \in \mathbb{C}$, 1 is an identity for G.
3. G is closed under inverses. We know the multiplicative inverse of z is the complex number $1/z$, so we just need to check that $1/z \in G$. If $z \in G$, $z^n = 1$ for some $n \in \mathbb{Z}^+$. Then, $(1/z)^n = 1$ as well, so $1/z \in G$.
4. G is associative. If $a, b, c \in G$, then $a, b, c \in \mathbb{C}\backslash\{0\}$ and by the associativity of $(\mathbb{C}\backslash\{0\}, \times)$, $a(bc) = (ab)c$.

Exercise 1.1.9b

Let $G = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$. Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators to find multiplicative inverses.]

Let H be the set of nonzero elements of G. There are four things to check:

1. H is closed under multiplication. If $a + b\sqrt{2} \in H$ and $c + d\sqrt{2} \in H$, then they are both nonzero, so their product is also nonzero. Their product can be written as
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$
If $a, b, c, d \in \mathbb{Q}$, the quantities $ac + 2bd$ and $ad + bc$ also lie in $\mathbb{Q}$, so this product lies in H.
2. H contains an identity. The identity is the real number $1 = 1 + 0\sqrt{2}$. Because $1 \cdot r = r$ for any $r \in \mathbb{R}$, 1 is an identity for H.
3. H is closed under inverses. Let $r = a + b\sqrt{2} \in H$. Then, $r \neq 0$, so either $a \neq 0$ or $b \neq 0$, so $a - b\sqrt{2} \neq 0$ as well. Also, $a^2 - 2b^2 = (a - b\sqrt{2})(a + b\sqrt{2}) \neq 0$. Thus, we can compute the inverse of $a + b\sqrt{2}$ in $\mathbb{R}$:
$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}. \end{aligned}$$
This is an element of H because $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are both rational if $a, b \in \mathbb{Q}$.

4. H is associative. If $a, b, c \in H$, then $a, b, c \in \mathbb{R}\setminus\{0\}$, so by the associativity of $(\mathbb{R}\setminus\{0\}, \times)$, $a(bc) = (ab)c$.

Exercise 1.1.26

Assume H is a nonempty subset of $(G, \star)$, which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, $h \star k$ and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

There are four things to check:

1. H is closed under the operation $\star$. This is given.
2. H contains an identity. Let 1 be the identity of $(G, \star)$. Since H is nonempty, pick an element $h \in H$. We know that H is closed under inverses, so $h^{-1} \in H$. We also know that H is closed under $\star$, so $h \star h^{-1} = 1 \in H$. Because 1 is the identity of G, $1 \star h = h$ for all $h \in H$, so 1 is an identity of H.
3. H is closed under inverses. This is given.
4. H is associative. If $a, b, c \in H$, then $a, b, c \in G$, so by the associativity of $(G, \star)$, $a \star (b \star c) = (a \star b) \star c$.

Question 1

Give me an example of a group that you came up with yourself (didn't find in the textbook, or Wikipedia, etc.) You do need to specify the operation, but you do not need to prove it is a group (although if it turns out not to be a group, we won't be able to give you many points).

You get 1 bonus point if no other student submits the same group.

[Many different answers possible.]

Question 2

Let $G = \mathbb{R} \setminus \{0\}$ be the group of nonzero real numbers under multiplication, and let $H = \mathbb{C} \setminus \{0\}$ be the group of nonzero complex numbers under multiplication. (You don't need to prove these are groups).

Prove that G and H are *not* isomorphic.

Here is one possible argument:

Suppose for the sake of contradiction that there exists an isomorphism $f : H \to G$. We first check that $f(1) = 1$; this is in fact true for any *homomorphism* f. (We'll write 1_H and 1_G for clarity, but you did not have to do this.) Let $y = f(1_H)$; our goal is to show that $y = 1_G$. Since $1_H \cdot 1_H = 1_H$, we have

$$y \cdot y = f(1_H) \cdot f(1_H) = f(1_H \cdot 1_H) = f(1_H) = y$$

Multiplying both sides by y^{-1}, we conclude that

$$\begin{aligned} y^{-1} \cdot y \cdot y &= y^{-1} \cdot y \\ y &= 1_G \end{aligned}$$

Therefore $f(1_H) = 1_G$, as claimed.

Now, let $x = f(i)$. Since $i^4 = 1$ in H, and f is a homomorphism, $x^4 = f(i)^4 = f(i^4) = 1$ in G. The only real numbers x which satisfy $x^4 = 1$ are $x = \pm 1$. Either way, $x^2 = 1$. But

$$\begin{aligned} x^2 &= f(i)^2 \\ &= f(i^2) \\ &= f(-1), \end{aligned}$$

so $f(-1) = 1$. It follows that $f(1) = 1$ and $f(-1) = 1$ and f cannot be a bijection. This contradicts the fact that f is an isomorphism, so we're done.

(Another way to phrase this argument, now that we know about the *order* of an element, would be to say: $i \in H$ has order 4, so under an isomorphism it must go to an element of G with order 4. But there *are* no elements of order 4 in G.)

In general, it suffices to find a property that is preserved by isomorphisms which is true of H but not of G (or vice versa). For example:

- G only has two elements of finite order (namely 1 and -1). But H has infinitely many elements of finite order (namely all the roots of unity from 1.1.8a). [You really only need to show there are more than two, which you can do by just checking that i and $-i$ have finite order.]
- By the fundamental theorem of algebra[1], every element z of H is a square of some element in H (i.e. there exists an element $y \in H$ satisfying $y \cdot y = z$). But this is not true of G (since e.g. -4 is not a square of any element of G).

Question 3

We will call an element $g \in G$ an *involution* if $g^2 = 1$ but $g \neq 1$.

Let G be a finite group.

A. Suppose that G has an even number of elements. Show that G contains an involution. (Hint: can you show the set $X = \{x \in G | x^2 \neq 1\}$ has an even number of elements?)

Let $X = \{x \in G | x^2 \neq 1\}$. We begin by showing that every element x of X satisfies $x \neq x^{-1}$. By definition, any $x \in X$ satisfies $x^2 \neq 1$. Multiplying by x^{-1} on both sides,

$$\begin{aligned} x^{-1}(x^2) &\neq x^{-1}(1) \\ x &\neq x^{-1}, \end{aligned}$$

Thus, every element of X is different from its inverse. Pair up every element $x \in X$ with its inverse x^{-1}. Note this is a *different* element, by our argument above that $x \neq x^{-1}$. Moreover, x^{-1} is paired with $(x^{-1})^{-1} = x$ again. So we have paired up the elements of X into disjoint two-element sets $\{x, x^{-1}\}$. Therefore X must be even in total size (since its size is twice the number of pairs).

Because X and G both have an even number of elements, the complement $G \setminus X$ of X in G also has an even number of elements (since $|G| = |X| + |G \setminus X|$).

But $G \setminus X$ contains 1 (since $1^2 = 1$), so its size is ≥ 1. So if $G \setminus X$ has even size, it must contain at least two elements. Pick any element g of $G \setminus X$ other than 1; it must satisfy $g^2 = 1$, so it's an involution, as desired.

B. (Optional) Conversely, show that if G contains an involution g, then G contains an even number of elements.

Let $g \in G$ be an involution. Pair up every element $x \in G$ with the element gx. Note that since $g \neq 1$, this is a *different* element ($x \neq gx$). Moreover, gx will be paired with $g^2 x = x$ again. So we have paired up the elements of G into disjoint two-element sets $\{x, gx\}$. Therefore G must be even in size (since its size is twice the number of pairs).

Question 4

(Optional) You may know that real numbers can have at most two square roots. The same is true of complex numbers. Is this true in groups?

The claim is false. We prove this by giving a counterexample group.

Fix some $n \geq 2$, and let G be the group of length-n binary strings, where the group operation is XOR. There are 2^n elements of this group.

Since the group operation is XOR, a "square root" of a string h is any g such that g XOR $g = h$. But g XOR g is always equal to 000000 no matter what g is! Therefore 000000 has 2^n square roots (and no other element has *any* square roots).

[1] The fundamental theorem of algebra says that every polynomial with complex coefficients has at least one root in $\mathbb{C}$.