Problem Set 1
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 11, 2018

Section 1.1

Ex 7 Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x * y$ be the fractional part of $x + y$. Prove that $*$ is a well defined binary operation on G and that G is an abelian group under $*$.

Proof.

a) (Well-defined) Let $x, y \in G$. Then $x * y = x + y - [x + y]$, where $[\cdot]$ is the greatest integer less than $x + y$. We see that it must that $0 \leq x + y - [x + y] < 1$, otherwise there'd be an integer between $[x + y]$ and $x+y$, contradiction our definition of $[\cdot]$. Thus $x * y \in G$.

b) (Associativity) Let $\phi(r) = r - [r]$. Note that the binary operation $x * y$ is equivalent to $\phi(x + y)$. I claim that $\phi(x + \phi(y)) = \phi(x + y)$. Here's the proof: let $\phi(y) = r$. Then $y = r + n$ for some $n \in \mathbb{Z}$. Thus, my claim is equivalent to $\phi(x + r) = \phi(x + r + n)$, which is true as adding an integer doesn't alter the fractional part. Thus, using this multiple times we see that $x * (y * z) = \phi(x + \phi(y + z)) = \phi(x + y + z) = \phi(\phi(x + y) + z) = (x * y) * z$. This proves associativity.

c) (Commutativity) We see that $x * y = x + y - [x + y] = y + x - [y + x] = y * x$.

d) (Identity) We can see that $0 \in G$ and that for every $x \in G$, $[x] = 0$ as $0 \leq x < 1$. This means that $x * 0 = x + 0 - [x + 0] = x - [x] = x$. Since we've already proven commutativity, we know that $0 * x = x$ as well.

e) (Inverses) Let $0 \neq x \in G$. Since $0 < x < 1$, we have that $0 < 1 - x < 1$, which proves that $1 - x \in G$. Additionally, we can see that $x * (1 - x) = x + (1 - x) - [x + (1 - x)] = 1 - [1] = 0$. Since we've already proved commutativity, this means that for $x \neq 0$, $1 - x$ is its inverse. If $x = 0$, then we can easily see that itself serves as its inverse. $\square$

Ex 8 Let $G = \{z \in \mathbb{C} \mid z^n = 1\}$ for some $n \in \mathbb{Z}^+$.

a) Prove that G is a group under multiplication

b) Prove that G is not a group under addition

Proof.

a) Since G is a subset of $\mathbb{C}$ which is a group under multiplication, we need only to check that G is non-empty and that for $x, y \in G$ we have that $xy^{-1} \in G$. One can see that $1 \in G$ as $1^1 = 1$, so G is non-empty. Now suppose $x, y \in G$. This means that $x^n = 1$ and $y^k = 1$ for some $n, k \in \mathbb{Z}^+$. Thus, since multiplication over complex numbers is commutative, we have that $(xy^{-1})^{nk} = (x^n)^k \left(y^k\right)^{-n} = 1^k 1^{-n} = 1$. Thus, G is a group.

b) Look at the element $1 \in G$. We see that $1 + 1 = 2$ (Hopefully!). However, $2^n \neq 1$ for any $n \in \mathbb{Z}^+$. Thus, G is not closed under addition. $\square$

Ex 9 Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

a) Prove that G is a group under addition

b) Prove that the nonzero elements of G are a group under multiplication

Proof.

a) Since G is a subset of $\mathbb{R}$ and $\mathbb{R}$ is a group under addition, we need only to check that G is non-empty and that for $x, y \in G$, we have that $x - y \in G$. We easily see that $0 + 0\sqrt{2} = 0 \in G$, so G is non-empty. Suppose now that $x, y \in G$. This means that $x = a + b\sqrt{2}$ and that $y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$. This means that $x - y = a + b\sqrt{2} - c - d\sqrt{2} = (a - c) + (b - d)\sqrt{2} \in G$. This proves that G is a group under addition.

b) Similar to the first part, we first see that $1 + 0\sqrt{2} = 1 \in G^\times$, which proves that $G^\times$ is non-empty. Now we suppose that $x, y \in G$. This means that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$, where $g \neq 0 \neq h$. Thus,

$$\begin{aligned} x \cdot y^{-1} &= \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} \\ &= \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - d^2} = \frac{ac - 2bd}{c^2 - 2d^2} - \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}. \end{aligned}$$

We see that since $x, y \in G^\times \subseteq \mathbb{R}^\times$, it cannot be that $xy^{-1} = 0$. Now we need only to prove that $c^2 - 2d^2 \neq 0$. By way of contradiction, assume that $c^2 = 2d^2$. This would mean that $\frac{c}{d} = \sqrt{2}$, which is impossible as $c, d \in \mathbb{Q}$ and $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. Thus, xy^{-1} is well-defined, non-zero, and has rational coefficients, which proves that $xy^{-1} \in G^\times$ as required. $\square$

Ex 20 For x an element in G show that x and x^{-1} have the same order.

Proof. Assume that the order of x is n, that the order of x^{-1} is k, and that $n \neq k$. Without loss of generality, we assume that $0 < n < k$. We see that

$$(g^{-1})^n = (g^n)^{-1} = 1^{-1} = 1$$

which is a contradiction as k was assumed to be the smallest natural number such that $(g^{-1})^k = 1$. Thus, it must be that $n = k$. $\square$

Ex 22 If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof. We first note that

$$(g^{-1}xg)^k = g^{-1}xg \cdot g^{-1}xg \cdot \dots \cdot g^{-1}xg = g^{-1}x^k g$$

for any natural number k. Suppose that the order of x is n and that the order of $g^{-1}xg$ is m. We see then that $(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}g = 1$, which proves that $k \leq n$. Since $(g^{-1}xg)^m = g^{-1}x^m g = 1$, then if we multiply on the right by g and on the left by g^{-1}, we obtain that $x^m = gg^{-1} = 1$. This proves that $n \leq k$ and thus that $n = k$. If we let $x = ab$ and $g = a$, then we have that $|ab| = |a^{-1}aba| = |ba|$ as desired. $\square$

Ex 27 Prove that if x is an element of the group G then $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup.

Proof. We first note that H is a subset of G and that G is a group. We see that H is non-empty as $x = x^1 \in H$. Suppose now that $a, b \in H$. Then we have that $a = x^n$ and that $b = x^m$ for some $n, m \in \mathbb{Z}$. Thus, we have that $ab^{-1} = x^n x^{-m} = x^{n-m} \in H$. This proves that H is a subgroup of G. $\square$

Ex 32 If x is an element of finite order n in G, prove that the elements $1, x, x^2, \dots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$

Proof. By way of contradiction, suppose that these elements are not distinct. Without loss of generality, this means that $x^\ell = x^k$ for some $0 \leq \ell < k \leq n-1$. We see that if multiply both sides by $x^{-\ell}$ we have that $1 = x^{\ell-\ell} = x^{k-\ell}$. However, $0 < k - \ell < n$ and n was assumed to be the smallest natural number such that $x^n = 1$. This is a contradiction, which proves that these elements must be distinct. If one lets A be the set of these elements, then we see that $|A| = |x| = n$. Since $A \subseteq G$, we have that $|x| = |A| \leq |G|$ as desired. $\square$

Ex 36 Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4. Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Proof. By Lagrange's Theorem, the order of each element must divide the order of the group, which in this case is 4. Since no element has order 4 by assumption and the only element of order 1 is the identity, we can deduce that a, b, c all have order 2. Now we look at the element ab. We see that if $ab = a$ or $ab = b$ we could use the cancellation laws to prove that $b = 1$ or $a = 1$ respectively, which is a contradiction. If $ab = 1$, then a and b would be inverses of each other. This is also a contradiction as since a and b each have order 2, their unique inverses are themselves. Thus, it must be that $ab = c$. By using a similar argument, we can deduce that $ab = ba = c$, $ac = ca = b$, and that $bc = cb = a$. This means that the group table of G is uniquely defined and that G is abelian. $\square$

Section 1.6

Ex 1 Let $\varphi : G \to H$ be a homomorphism.

a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$

b) Prove that $\varphi(x^{-1}) = \varphi(x)^{-1}$ and extend the result of part (a) to all $n \in \mathbb{Z}$

Proof.

a) We will prove this via induction. If $n = 1$, then we have that $\varphi(x) = \varphi(x)$, which is trivially true. Now let's look at $n + 1$. Using the induction hypothesis, we see that

$$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$$

which proves the statement.

b) This time we will prove the statement for all negative integers via induction. As our base case, we see that $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H$, which proves that $\varphi(x^{-1}) = \varphi(x)^{-1}$ as desired. Now let's look at $-(n+1)$. Using the inductive hypothesis and our base case, we see that

$$\varphi(x^{-(n+1)}) = \varphi(x^{-n}x^{-1}) = \varphi(x^{-n})\varphi(x^{-1}) = \varphi(x)^{-n}\varphi(x)^{-1} = \varphi(x)^{-(n+1)}$$

which proves the statement for all negative integers. If we combine this with part (a) and with the fact that $\varphi(x^0) = \varphi(1_G) = 1_H = \varphi(x)^0$, we have the statement for all integers. $\square$

Ex 2 If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if ϕ is only assumed to be a homomorphism?

Proof. Suppose that the order of x is n. We see then that $\varphi(x)^n = \varphi(x^n) = \varphi(1_G) = 1_H$, which proves that $|\varphi(x)| \leq n$. By contradiction, assume that that $0 < |\varphi(x)| = k < n$. This would mean that $\varphi(x)^k = \varphi(x^k) = 1_H$. Since φ is an isomorphism, its kernel is $\{1_G\}$. Thus, $x^k = 1_G$, which is a contradiction as the order of x is n and $0 < k < n$. This proves that $|x|$ and $|\varphi(x)|$ must have the same order.

Now suppose that G and H had a differing number of elements of order n. Without loss of generality, let H be the group with the fewer number of elements of order n. This would mean that if we let $S = \{g \in G : |g| = n\}$, then $|\varphi(S)| < |S|$, as every element has to be mapped to an element of the same order and there are fewer such elements in H. This contradicts the fact that φ is injective. Thus, two isomorphic groups must have the same number of elements of order n.

The statement is not true if φ is only assumed to be a homomorphism. To see this, take the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ where φ is the parity function. In the group $\mathbb{Z}/2\mathbb{Z}$ there are only two elements, one of order 1 and another of order 2. However in the group $\mathbb{Z}$, all elements except the identity have infinite order, as the only solution to $g^n = ng = 0$ for $n \in \mathbb{Z}^+$ is when $g = 0$. Thus, the result does not extend to homomorphisms. $\square$

Ex 4 Prove that the multiplicative groups $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic.

Proof. By Ex 2, we know that if the two groups were isomorphic, then they should have the same number of elements of order 4. However, $\mathbb{R}$ has zero elements of order 4 and $\mathbb{C}$ has at least one, namely i. Thus, these groups are not isomorphic. $\square$

Ex 9 Prove that D_{24} and S_4 are not isomorphic.

Proof. First, we will prove that any element of S_4 has order at most 4. To do this, suppose that σ is a cycle in S_4. Since S_4 is the set of permutations on a 4-element set, we can deduce that σ is at most a 4-cycle. This proves that σ has at most order 4. Now suppose that σ is not a cycle in S_4. This means that σ is either the identity or the product of two disjoint 2-cycles. The identity element always has order 1 and the product of two disjoint 2-cycles has order 2. This proves that the order of any element of S_4 is at most 4. Furthermore, we note that the element $r \in D_{2n}$ has order n, which means that r has order 12 in D_{24}. If there were an isomorphism $\varphi : D_{24} \to S_4$, then this would mean that $|\varphi(r)|$ would have order 12 as well. This is impossible, as we proved that there exists no such element in S_4. Thus, D_{24} and S_4 cannot be isomorphic. $\square$

Ex 10 Let $\theta : \Delta \to \Omega$ be a bijection. Define $\varphi : S_\Delta \to S_\Omega$ by $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ for all $\sigma \in S_\Delta$ and prove the following:

a) φ is well-defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω

b) φ is a bijection from S_Δ onto S_Ω

c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$

Proof.

a) Suppose that σ is a permutation of Δ, that is, σ is a bijection from Δ to Δ. Since we know that θ is a bijection from Δ to Ω, we see that $\theta \circ \sigma \circ \theta^{-1}$ is a bijection from $\Omega \to \Delta \to \Delta \to \Omega$. Since this is a bijection from Ω to Ω, we can deduce that $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

b) We define $\psi : S_\Omega \to S_\Delta$ by $\psi(\omega) = \theta^{-1} \circ \omega \circ \theta$. We see that

$$\psi(\varphi(\sigma)) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = 1 \circ \sigma \circ 1 = \sigma$$
$$\varphi(\psi(\omega)) = \theta \circ (\theta^{-1} \circ \sigma \circ \theta) \circ \theta^{-1} = 1 \circ \omega \circ 1 = \omega$$

which means that ψ and φ are inverses. Thus, φ is a bijection.

c) This is shown by the following:

$$\varphi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \varphi(\sigma) \circ \varphi(\tau).$$ $\square$

Ex 14 Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Define the kernel of ϕ to be $\{g \in G \mid \phi(g) = 1_H\}$. Prove that the kernel of ϕ is a subgroup of G. Prove that ϕ is injective if and only if the kernel of ϕ is the identity subgroup of G.

Proof. We note that the kernel is a subset of G which is a group. We also see that the kernel is always non-empty as $\varphi(1_G) = 1_H$. Suppose that $x, y \in \ker(\varphi)$. This means that $\varphi(x) = 1_H = \varphi(y)$, which we can use to show that

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1} = 1_H.$$

This proves that $xy^{-1} \in \ker(\varphi)$, which means that $\ker(\varphi)$ is a subgroup of G.

To prove the second part of the exercise, suppose that φ is injective and that $g \in \ker(\varphi)$. Since $\varphi(1_G) = 1_H = \varphi(g)$ and φ is injective, this proves that $g = 1_G$. Thus, $\ker(\varphi) = \{1_G\}$, the identity subgroup. Now conversely, suppose that $\ker(\varphi) = \{1_G\}$ and that $\varphi(x) = \varphi(y)$ for some $x, y \in G$. As φ is a homomorphism, this means that $\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) = 1_H$. However, 1_G is the only element in $\ker(\varphi)$, which means that xy^{-1} must be 1_G. From this we can easily see that $x = y$, which proves that φ is injective. $\square$

Ex 17 Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. Let φ be such a map. If G is abelian, then

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$$

which proves that φ is a homomorphism. Now conversely assume that φ is a homomorphism. This means that

$$(xy)^{-1} = \varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1} = (yx)^{-1}.$$

If we take the inverse of both sides, then we obtain that $xy = yx$ as desired. $\square$

Additional Problems

Ex A Let $\phi : (G, \cdot) \to (H, *)$ be a group homomorphism. Prove that $\phi(e_G) = e_H$.

Proof. We see that

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) * \varphi(e_G).$$

Using cancellation, this means that $e_H = \varphi(e_G)$ as desired. $\square$

Ex B Let $\pi : (G, \cdot) \to (G, \cdot)$ be given by $\pi(g) = g^{-1}$. Prove that π is an anti-homomorphism. Also prove that π is a bijection.

Proof. We see that

$$\pi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \pi(h)\pi(g)$$

which proves that π is an anti-homomorphism. If we let $\pi(g) = \pi(h)$, then we have that $g^{-1} = h^{-1}$. By multiplying on the right by g and on the left by h, we have that $h = g$, which proves that π is injective. We also see that for all $g \in G$, we have that $\pi(g^{-1}) = (g^{-1})^{-1} = g$. This proves that π is surjective, which means that π is a bijection. $\square$