Problem Set 1
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 15, 2018

Lemma : A subset, H, of a group, G, is a subgroup iff $H \neq \varnothing$ and $g, h \in H \implies gh^{-1} \in H$ are satisfied. These two latter criteria will be referred to as the two-step subgroup criteria throughout the rest of this homework.

Proof. Let $H \leq G$. Then, H is a group, so it must contain the identity, so that means $H \neq \varnothing$. Let $g, h \in H$. Also, H is closed under inverses, so this means that $h^{-1} \in H$. And again, since H is closed under the group operation, this means that $g \cdot h^{-1} \in H$. Thus, H satisfies the two critiera test.

Say H satisfies the two-step critiera test. This means that H is nonempty. Let $x \in H$. Since for all $g, h \in H$, then $gh^{-1} \in H$, this means if we let $g = h = x$, then $xx^{-1} = 1 \in H$. Thus, H contains the identity. Now let $g = e$ and $h = x$, this means that $ex^{-1} = x^{-1} \in H$. Thus, H is closed under inverses. Finally, let $x, y \in H$. This means that $y^{-1} \in H$ as well. Thus, if we let $g = x$ and $h = y^{-1}$, we get that $x\left(y^{-1}\right)^{-1} = xy \in H$. Thus, H is closed under the group operation. Since $H \subseteq G$, H is also associative. Therefore, $H \leq G$. □

Section 1.1

Exercise 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 $x * y = x + y - [x + y]$. Since $[x + y]$ is the greatest integer such that $[x + y] < x + y$, it must that $0 \leq x + y - [x + y] < 1$, otherwise there'd be an integer between $[x + y]$ and $x + y$. 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 $x \in G$, $x * 0 = x + 0 - [x + 0] = x - [x] = x$, as $0 \leq x < 1$ already, which means $[x] = 0$. Since we've proven commutativity, we know that $0 * x = x$ as well.

e) (Inverses) Let $0 \neq x \in G$. Since $0 < x < 1$, then $-1 < -x < 0$, which means $0 < 1 - x < 1$. Thus, $1 - x \in G$. We can see that $x * (1 - x) = x + (1 - x) - [x + (1 - x)] = 1 - [1] = 0$, as $[1] = 1$. Thus $(1 - x)$ is the inverse of $x \neq 0$. (It's two-sided, as G is commutative.) If $x = 0$, then the inverse is, of course, itself.

□

Exercise 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 $G \subseteq \mathbb{C}$, we need only to check that $(G, \cdot) \leq (\mathbb{C}, \cdot)$. One can see that $1 \in G$ as $1^1 = 1$. If $x, y \in G$, then $x^n = 1$ and $y^k = 1$ for some $n, k \in \mathbb{Z}^+$. Thus, $(xy^{-1})^{nk} = (x^n)^k \left(x^k\right)^n = 1^k 1^n = 1$. ($(xy)^n = xyxy \dots xy = x \dots x \cdot y \dots y = x^n y^n$ as G is commutative.) 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.

□

Exercise 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) We see that $(G, +) \subseteq (\mathbb{R}, +)$. Thus, to prove that G is a group, we only need to check the subgroup criteria.

Nonempty) This is easy, as $0 + 0\sqrt{2} = 0 \in G$

Closure) Let $g, h \in G$, then $g = a + b\sqrt{2}$ and $h = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$. Thus, $g - h = a + b\sqrt{2} - c - d\sqrt{2} = (a - c) + (b - d)\sqrt{2} \in G$.

b) Again, we see that $(G^\times, \cdot) \subseteq (\mathbb{R}^\times, \cdot)$, and thus we only need to check the subgroup criteria.

Nonempty) Easy. We see that $1 + 0\sqrt{2} = 1 \in G^\times$.

Closure) Let $g, h \in G$, then $g = a + b\sqrt{2}$ and $h = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$, where $g \neq 0 \neq h$. Thus, $g \cdot h^{-1} = \left(a \cdot b\sqrt{2}\right) \cdot \frac{1}{c + d\sqrt{2}} = \frac{a \cdot b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right)\left(c - d\sqrt{2}\right)}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} - \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}$. We can see this is well-defined and nonzero by looking that if $c^2 = 2d^2$, then $\frac{c^2}{d^2} = 2$, which would mean $\left(\frac{c}{d}\right)^2 = 2$, and finally that $\frac{c}{d} = \sqrt{2}$, which is impossible as c, d are in $\mathbb{Q}$ and $\sqrt{2}$ is in $\mathbb{R} \backslash \mathbb{Q}$. Now it remains to prove that it's nonzero. Assume $bc = ad$

(that is, the second term is zero). Multiplying by $d^{-1}c$, we get $bc^2d^{-1} = ac$. If the first term were also zero, then this would mean $bc^2d^{-1} = ac = 2bd$. Multiplying by db^{-1}, we get $c^2 = 2d^2$. We already proved before that this is impossible. This, $\frac{ac-2bd}{c^2-2d^2} - \frac{bc-ad}{c^2-2d^2}\sqrt{2}$ is a well-defined, nonzero element in G. This proves that G is a group under multiplication. □

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

Proof. Assume that the order of g is n, that the order of g^{-1} is k, and that they are distinct. Let $n < k$ without less of generality (as g^{-1} is also the inverse of g). Then $g^n = 1$. Multiplying both sides by $(g^n)^{-1}$, we see that $(g^n)^{-1} g^n = (g^n)^{-1} 1$. This shows that $1 = (g^n)^{-1} = (g^{-1})^n$. However, k was assumed to be the least such natural number that satisfies the equation $(g^{-1})^k = 1$. This is a contradiction and thus, $n = k$. □

Exercise 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. Claim: $\phi_g : G \to G : x \mapsto g^{-1}xg$ is a isomorphism. It's a homomorphism as $\phi_g(ab) = g^{-1}abg = g^{-1}agg^{-1}bg = \phi_g(a)\phi_g(b)$. It's injective as if $\phi_g(a) = \phi_g(b)$, then that means $g^{-1}ag = g^{-1}bg$. Right cancel and left cancel to get $a = b$. It's surjective, as for $b \in G$, let $a = gbg^{-1} \in G$. This means that $\phi(a) = \phi(gbg^{-1}) = g^{-1}gbg^{-1}g = 1b1 = b$. Thus, by Sec 1.6 Ex 2, $|x| = |\phi_g(x)| = |g^{-1}xg|$. This means that $|ab| = |\phi_a(ab)| = |a^{-1}aba| = |ba|$. □

Exercise 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. a) (Non-empty) $x = x^1 \in H$.

b) (Closure) Let $g, h \in H$. Then $g = x^n$ and $h = x^k$ for some $n, k \in \mathbb{Z}$. Thus, $gh^{-1} = x^n \left(x^k\right)^{-1} = x^n x^{-k} = x^{n-k} \in G$

□

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

Proof. Say that the elements are not distinct. Then $x^l = x^k$ for some $0 \leq l, k < n$ and $l \neq k$. Assume, without loss of generality, that $l < k$. Then, if one multiplies both sides by x^{-1} l times, we get $1 = x^{l-l} = x^{k-l}$. But, $k - l < n$, and n was assumed to be the least such integer satisfying $x^n = 1$. This is a contradiction, and thus the elements must be distinct. If you let A equal the set of those elements, than $|A| = n$, as they're all distinct. Since $A \subseteq G$, we see that $|x| = |A| \leq |G|$. □

Exercise 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. If no element has an order of 4 and the identity is the only element of order 2, and by Lagrange's Theorem, the order of an element divides the order of the group, we can see that the order of a, b, c are all 2. Look at ab. We see that $ab = c$, as if $ab = a$ or $ab = b$, then you could cancel and see that b or a is the identity respectively, which is a contradiction. ab also can't equal 1, as that would mean that they're inverses, and since the order of a and b is 2, $a^2 = aa = 0$ and $b^2 = bb = 0$, so their unique inverses have already been determined to not be each other. This proves that $ab = c$. A similar argument can be made for $ba = c$ and the various combinations of pairwise multiplication of a, b, c. Thus, there is a unique group table for G.

We can see that G is abelian as if you look above we deduced that $ab = c = ba$, this follows with other pairwise combinations of a, b, c, and since $1 \in Z(G)$ for any group G, 1 commutes with everything anyway. Thus, all possible multiplications that can be done in G are communtative. □

Section 1.6

Exercise 1. Let $\phi : G \to H$ be a homomorphism.

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

b) Do part (a) for $n = -1$ and deduce that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$

Proof. a) (Proof by Induction)
Case $n = 1$)
If $n = 1$, then we see that $\phi(x) = \phi(x)$. This is, of course, trivally true.
Case $n = k + 1$)
We see that $\phi\left(x^{k+1}\right) = \phi\left(x^k x\right) = \phi\left(x^k\right)\phi(x)$. By the induction hypothesis: $\phi\left(x^k\right) = \phi(x)^k$. Thus, $\phi\left(x^{k+1}\right) = \phi\left(x^k\right)\phi(x) = \phi(x)^k\phi(x) = \phi(x)^{k+1}$. Thus, by induction, we have proven that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}^+$.

b) (Proof by Induction)
Case $n = -1$)
$\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1_G) = 1_H$. Thus, $\phi(x^{-1})$ is the inverse of $\phi(x)$.
Case $n = -k - 1$)
If $\phi\left(x^{-k-1}\right) = \phi(x^{-k}x^{-1}) = \phi\left(x^{-k}\right)\phi(x^{-1}) = \phi(x)^{-k}\phi(x)^{-1} = \phi(x)^{-k-1}$, since $\phi\left(x^{-k}\right) = \phi(x)^{-k}$ according to the inductive hypothesis. Thus, $\phi(x^{-n}) = \phi(x)^{-n}$. This combined with the knowledge that $\phi(1_G) = 1_H$, we see that $\phi(x^n) = \phi(x)^n$ for all n in $\mathbb{Z}$.

□

Exercise 2. If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ 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. Say that $|x| = n$. Then this means that $x^n = 1$. Then this means that $1_H = \phi(1_G) = \phi(x^n) = \phi(x)^n$. So $|\phi(x)| \leq n$. Say that $|\phi(x)| = k < n$. Then $\phi(x)^k = 1_H$, which would mean that $\phi(x)^k = \phi\left(x^k\right) = 1_H$. Since ϕ is a isomorphism, its kernel is only $\{1_G\}$. Thus, $x^k = 1_G$. This is a contradiction, as n was assumed to be the least such. Thus $|\phi(x)| = n$.

Assume that two isomorphic groups had a different number of elements of order n for an $n \in \mathbb{Z}^+$. Without loss of generality, let H be the group with lesser elements of order n. Now, let $S = \{g \in G \mid |g| = n\}$. This means that $|\phi(S)| < |S|$, as every element has to be mapped to an element of the same order in H, but there aren't as many elements of that order in H. This contradicts that ϕ is injective. Thus, two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

This is not true if ϕ is only assumed to be a homomorphism. Take the homomorphism $\phi : \mathbb{Z} \to \{0, 1\}$, where ϕ is the parity function (that is, it's one if the input is odd and zero if the input is even). In the target group there are only two elements, one of order 1, as it's the identity, and one of order 2. However, in $(\mathbb{Z}, +)$, all elements except the identity have infinite order, as the only solution to $ng = 0$ for $n \in \mathbb{Z}^+$ and $g \in (\mathbb{Z}, +)$ is when $g = 0$. Thus, the result is not true if ϕ is only a homomorphism. □

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

Proof. By (Sec 1.6 Ex 2), we see that if the two groups were isomorphic, then they zould have the same number of elements of order 4. However, $\mathbb{R}$ has no element of order 4, and $\mathbb{C}$ does have one, namely i. Thus, they are not isomorphic. □

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

Proof. There are 12 elements in D_{24} that have order of 2. These are the elements of the form sr^i for $0 \leq i < 12$. These have order two as $sr^i sr^i = ssr^{-i}r^i = ssr^0 = ss = 0$, as the order of s is two. Let σ be a permutation of S_4. It can only have an order of 2 if it just switches two elements with each other. There are 4 choose 2 such combinations that are possible, which is equal to 6. Thus, by Sec 1.6 Ex 2, since the two groups have a differing number of elements of order 2, this means the groups are not isomorphic. □

Exercise 10. Let $\theta : \Delta \to \Omega$ be a bijection. Define
$\phi : S_\Delta \to S_\Omega$ by $\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ 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 [Find a 2-sided inverse for ϕ]

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

Proof. a) A permutation is just a bijection from a set onto itself. Thus, if σ is a permutation, that means that it's a bijection from $\Delta \to \Delta$. Since θ is a bijection from $\Delta \to \Omega$, this means that $\theta \circ \sigma \circ \theta^{-1}$ is a composition of bijective functions, which is bijective. Specifically, it's a bijection from $\Omega \to \Delta \to \Delta \to \Omega$. This means that $\theta \circ \sigma \circ \theta^{-1}$ is a bijection from $\Omega \to \Omega$. This shows that it's a permutation of Ω.

b) Let $\psi(\sigma) = \theta^{-1} \circ \sigma \circ \theta$. Then this means $\psi(\phi(\sigma)) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = 1 \circ \sigma \circ 1 = \sigma$. And also that $\phi(\psi(\sigma)) = \theta \circ (\theta^{-1} \circ \sigma \circ \theta) \circ \theta^{-1} = 1 \circ \sigma \circ 1 = \sigma$. Thus, ψ is the inverse of ϕ. This proves that ϕ is a bijection.

c) $\phi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = \theta \circ \sigma \circ 1 \circ \tau \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \phi(\sigma) \circ \phi(\tau)$
□

Exercise 14. Let G and H be groups and let $\phi : G \to$ 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. Well, firstly, the kernel is nonempty, as $\phi(1_G) = 1_H$ no matter what. Now, let $x, y \in \ker(\phi)$. This means $\phi(x) = 1_H = \phi(y)$. Thus $\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = 1_H 1_H^{-1} = 1_H$. Thus, $xy^{-1} \in \ker(\phi)$, which means $\ker(\phi)$ is a group.

If ϕ is injective and $g \in \ker(\phi)$, then since $1_G \in \ker(\phi)$, $\phi(g) = 1_H = \phi(1_G)$, which means $g = 1_G$. If $\ker(\phi) = \{1_G\}$, then if $\phi(x) = \phi(y)$, this means $\phi(x)\phi(y)^{-1} = 1_H$. Since ϕ is a homomorphism, then $\phi(x)\phi(y)^{-1} = \phi(xy^{-1}) = 1_H$. But only $\phi(1_G) = 1_H$. Thus $xy^{-1} = 1_G$, which means $x = y$. Thus ϕ is injective. □

Exercise 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 $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$. Thus the map is a homomorphism.

Now assume that ϕ is a homomorphism. Then $\phi(xy) = \phi(x)\phi(y)$. This means that $(xy)^{-1} = x^{-1}y^{-1}$. Multiply by xy on the left and yx on the right, then on the LHS, you get $xy(xy)^{-1}yx = 1yx = yx$ and on the RHS you get $xyx^{-1}y^{-1}yx = xyx^{-1}x = xy$. Thus, $yx = xy$, which proves that G is abelian. □

Additional Problems

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

Proof. We see that $\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) * \phi(e_G)$. Now, multiply both sides by $\phi(e_G)^{-1}$. Thus $\phi(e_G)^{-1} * \phi(e_G) = \phi(e_G)^{-1} * \phi(e_G) * \phi(e_G) \implies e_H = e_H * \phi(e_G) = \phi(e_G)$ □

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

Proof. We see that $\pi(gh) = (hg)^{-1} = h^{-1}g^{-1} = \pi(h)\pi(g)$. Thus, π is an antihomomorphism. Now we must prove that it is bijective. To check if it's injective, let $\pi(g) = \pi(h)$, which means $g^{-1} = h^{-1}$. If you multiply on the right by g and on the left by h, you get $g(g^{-1})h = g(h^{-1})h \implies eh = ge \implies h = g$. Thus, π is injective. To prove it's a surjection, we see that for all $g \in G$, $\pi(g^{-1}) = (g^{-1})^{-1} = g$. Thus, π is a surjection, and consequently, a bijection. □