Problem Set 3
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 2.1

Ex 4 Give an explicit example of a group G with an infinite subset H of G that is closed under the group operation, but is not a subgroup of G.

Proof. Let $G = (\mathbb{R}, +)$ and let $H = \{x \in \mathbb{R} \mid x \geq 0\}$. We see that $H \subseteq G$ and that if one takes two nonnegative real numbers and adds them together, the result is a nonnegative real number. However, H is not a subgroup of G, as H is not closed under inverses, i.e., if $x \in H$, then $-x \notin H$. □

Ex 5 Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Proof. By Legrange's Theorem, we see that $\frac{|G|}{|H|} \in \mathbb{N}$. Thus, this would mean that $\frac{n}{n-1} \in \mathbb{N}$. If $\frac{n}{n-1} = \frac{k}{1}$ for $k \in \mathbb{N}$, then by cross-multiplying, we get that $n = k\,(n-1)$. Suppose, $k = 1$, then $n = n - 1 \implies 0 = -1$, which is surely false. Thus, $k \geq 2$. We see that, though, $n = k\,(n-1) \geq 2\,(n-1) = 2n - 2$. Subtracting by n, we get that $0 \geq n - 2$, which means that $n \leq 2$. But, by assumption, $n > 2$. Thus, no such subgroup exists. □

Ex 6 Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a sub group when G is non-abelian.

Proof. Let $H = \{g \in G \mid |g| < \infty\}$. We see that if $g, h \in H$, then $|g| = n < \infty$ and that $|h| = k < \infty$. Since G is abelian, this means that $(g^{-1}h)^{nk} = g^{-nk}h^{nk} = (e^n)^{-k}\left(h^k\right)^n = 1^{-k}1^n = 1$. Thus, $g^{-1}h \in H$. We also see that $|e| = 1$, which implies that $e \in H$. Thus, by the two-step subgroup criteria proved on the first homework, H is subgroup of G.

Take D_∞, that is, the group generated by s and r with the presentation of $|r| = \infty$, $|s| = 2$, and $sr = r^{-1}s$. We see that $(sr)^2 = srsr = srr^{-1}s = ss = 1$. Thus, $|sr| = 2$, as e is the only element with order 1. Also, $|s| = 2$, by the presentation of D_∞. Thus, both of these elements are in H. However, $s \cdot sr = ssr = r$, which has order ∞. Thus, H is not closed under the operation. □

Ex 12 Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets of subgroups of A:

a) $\{a^n \mid a \in A\}$

b) $\{a \in A \mid a^n = 1\}$

Proof. a) Let $H = \{a^n \mid a \in A\}$. Since A is a group, this means that $1 \in A$, and since $1^n = 1$ for all $n \in \mathbb{N}$, this means that $1 \in H$. Let $g, h \in H$. This means that $g = a^n$ and $h = b^n$ for some $a, b \in A$. We see that since A is abelian that $g^{-1}h = (a^n)^{-1}(b^n) = (a^{-1})^n b^n = (a^{-1}b)^n$. Since A is a group, then $a^{-1}b \in A$. This shows that $g^{-1}h$ is in H. Thus, by the two-step subgroup criteria proved on the first homework, $H \leq A$.

b) Let $H = \{a \in A \mid a^n = 1\}$. Since A is a group, this means that $1 \in A$, and since $1^n = 1$, this means that $1 \in H$. Let $g, h \in H$. This means that $g^n = h^n = 1$. Thus, since A is abelian, we see that $(g^{-1}h)^n = g^{-n}h^n = (g^n)^{-1} h^n = 1^{-1}1 = 1$. Thus, $g^{-1}h \in H$. This means that by the two-step subgroup criteria proved on the first homework, $H \leq A$.

□

Ex 16 Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $\mathrm{GL}_n(F)$ (called the group of upper triangular matrices).

Proof. Didn't do. □

Ex 17 Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} \text{ for all } i\}$ is a subgroup of $\mathrm{GL}_n(F)$.

Proof. Didn't do. □

Section 2.2

Ex 1 Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Proof. Recall that the definition is that $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. Let $g \in C_G(A)$. Thus, $gag^{-1} = a$ for all $a \in A$. Multiplying on the left by g^{-1} and on the right by g, we get that $g^{-1}gag^{-1}g = g^{-1}ag$. After simplying, we get that $a = g^{-1}ag$ for all $a \in A$. Using a similar argument the other way around proves that $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\} = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$. □

Ex 2 Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Proof. By definition of C_G, we know that $C_G(Z(G)) \subseteq G$. Thus, to prove containment the other direction, let $g \in G$. By definition of C_G, we know that $g \in C_G(Z(G))$ if and only if $gag^{-1} = a$ for all $a \in Z(G)$. Multiplying by g on the right means that $ga = ag$ for all $a \in Z(G)$. However, by definition of $Z(G)$, all $a \in Z(G)$ commute with all elements of G, so $ga = ag$ is true. Thus, $g \in C_G(Z(G))$. This proves that $C_G(Z(G)) = G$.

We also see that if $x \in C_G(A)$, then $xax^{-1} = a$ for all $a \in A$. Thus $xax^{-1} = a \in A$, which means that $x \in N_G(A)$. This shows that $C_G(A) \subseteq N_G(A)$. By definition, $N_G(A) \subseteq G$. Thus, $C_G(Z(G)) = G \subseteq N_G(Z(G)) \subseteq G$. This proves that $N_G(Z(G)) = G$. □

Ex 5b Show that in the group $G = D_8$ with the subgroup $A = \{1, s, r^2, sr^2\}$ that $C_G(A) = A$ and that $N_G(A) = G$.

Proof. Since $C_G(A)$ is a subgroup of G, this means that $1 \in C_G(A)$. For easier compution, assume that the set A has a specific order. Then we see that $sAs^{-1} = s\{1, s, r^2, sr^2\}s = \{ss, sss, sr^2s, ssr^2s\} = \{1, s, ssr^{-2}, sssr^{-2}\} = \{1, s, r^2, sr^2\} = A$. Thus, $s \in C_G(A)$. We also see that $r^2Ar^{-2} = r^2\{1, s, r^2, sr^2\}r^2 = \{r^4, r^2sr^2, r^2r^2r^2, r^2sr^2r^2\} = \{1, sr^{-2}r^2, r^4r^2, sr^{-2}r^4\} = \{1, s, r^2, sr^2\} = A$. This means that $r^2 \in C_G(A)$. Since $C_G(A)$ is a group, this means that $sr^2 \in C_G(A)$. However, we see that $rsr^{-1} = rrs = r^2s \neq s$. This means that $r \notin C_G(A)$. Since, by Legrange's theorem, $|C_G(A)| \mid |G| = 8$, we see that $|C_G(A)|$ must be 1, 2, 4, or 8. We've proven that there are at least 4 elements in $C_G(A)$. Thus, $|C_G(A)|$ is either 4 or 8. If it were 8, then that'd mean that $C_G(A) = G$, but this is not true as $r \notin C_G(A)$. This means that $|C_G(A)| = 4$, and thus we've found all the elements in $C_G(A)$.

We know that $C_G(A) = A \leq N_G(A)$. This means that $|C_G(A)| = 4 \leq |N_G(A)| \leq |G| = 8$. We see that $r \cdot \{1, s, r^2, sr^2\} \cdot r^{-1} = \{rr^{-1}, rsr^{-1}, rr^2r^{-1}, rsr^2r^{-1}\} = \{1, sr^{-1}r^{-1}, r^{1+2-1}, sr^{-1}r^2r^{-1}\} = \{1, sr^{-2}, r^2, sr^{-1+2-1}\} = \{1, sr^2, r^2, s\} = A \subseteq A$. Thus, $r \in N_G(A)$. This means that $|N_G(A)| > |C_G(A)| = 4$. Since, $N_G(A)$ is a subgroup of G, and therefore by Legrange's Theorem, $|N_G(A)| \mid |G|$, this means that $|N_G(A)| = 1, 2, 4$ or 8. Since $|N_G(A)| > 4$, this means that $|N_G(A)| = 8 = |G|$. This proves that $N_G(A) = G$. ☐

Ex 7 Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

a) $Z(D_{2n}) = 1$ if n is odd

b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$

Proof. We proved in the last homework, in Sec 1.2 Ex 5, that the only element that commutes with all other elements in this group is the identity. Thus, $Z(G) = 1$.

We proved in the last homework, in Sec 1.2 Ex 4, that the only nonidentity element with commutes with all other elements of the group is r^k. Thus, $Z(G) = \{1, r^k\}$. ☐

Ex 12 Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are the finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$, where a is any integer and $r_1, \dots, r_4$ are nonnegative integers. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \dots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p\left(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}\right)$$

for all $p(x_1, x_2, x_3, x_4) \in \mathbb{R}$.

a) Let $p = p(x_1, \dots, x_4)$ be the polynomial $12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23}$ and let $\sigma = (1234)$ and let $\tau = (123)$. Compute $\sigma \cdot p$, $\tau(\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$ and $(\sigma \circ \tau) \cdot p$.

b) Prove that these definites give a group action of S_4 on R.

c) Exhibit all permutations in S_4 that stablize x_4 and prove that they form a subgroup isomorphic to S_3.

d) Exhibit all permutations in S_4 that stablize the element x_1+x_2 and prove that they form an abelian subgroup of order 4.

e) Exhibit all permutations in S_4 that stablize the element $x_1x_2+x_3x_4$ and prove that they form an abelian subgroup of order 8.

f) Show that the permutations in S_4 that stable the elment $(x_1+x_2)(x_3+x_4)$ are exactly the same as those found in part (e).

Proof. Please see the attached paper. □

Section 3.1

Ex 3 Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof. Let $xB, yB \in A/B$ where $x, y \in A$. Since A is abelian, then B is abelian, and is thus normal as well. We see that $xByB = xyB = yxB = yBxB$, as A is abelian and B is normal. Thus, B is abelian.

Recall that D_8 is not abelian. We proved in class that $H = \{1, r, r^2, r^3\}$ is a normal subgroup of D_8. Since $|H| = 4$ and $|D_8| = 8$, this means that $|G/H| = 2$. Thus, there are two elements in G/H. Let x be the nontrival element. We see that $x \neq 1 \implies x^2 \neq x$. Thus, x^2 must be the identity, the only other element in the group. This means that $1x = x1$, that $1 \cdot 1 = 1 \cdot 1$, and that $xx = 1 = xx$. Thus, this group must be abelian. □

Ex 6 Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Proof. The fibers of φ are $\varphi^{-1}(1) = \mathbb{R}^+$ and $\varphi^{-1}(-1) = \mathbb{R}^-$, that is the positive real numbers and negative real numbers respectively. We see that if $x, y \in \mathbb{R}^\times$, then $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{|x||y|} = \frac{x}{|x|}\frac{y}{|y|} = \varphi(x)\varphi(y)$. Thus, φ is a homomorphism. □

Ex 7 Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernal and fibers of π geometrically.

Proof. We see that if $(x, y), (a, b) \in \mathbb{R}^2$, then $\pi((x, y) + (a, b)) = \pi((x + a, y + b)) = x + a + y + b = x + y + a + b = \pi((x, y)) + \pi((a, b))$. Thus, π is a homomorphism. Let $r \in R$. We see that $(0, r)$ is in $\mathbb{R}^2$, and that $\pi((0, r)) = 0 + r = r$. This proves that π is surjective as well.

We also see that the fiber of an element $r \in R$, is all elements $(x, y) \in \mathbb{R}^2$, such that $\pi((x, y)) = x + y = r$. This means the fiber of $r \in R$ is the diagonal $(x, r - x)$. Specifically, for $r = 0$, we see that the kernel is the diagonal $(x, -x)$. Geometrically, this homomorphism linearly "compresses" $\mathbb{R}^2$ onto the diagonal (x, x). □

Ex 10 Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\bar{a}) = \bar{a}$. Show that this is a well-defined, surjective homomorphism and describe its fibers and kernel explicitly.

Proof. Recall that in $\mathbb{Z}/8\mathbb{Z}$, $\bar{r} = r + 8\mathbb{Z}$. Let $\bar{x}, \bar{y}$ be arbitrary elements in $\mathbb{Z}/8\mathbb{Z}$, where $\bar{x} = \bar{y}$. This means that $x + 8\mathbb{Z} = y + 8\mathbb{Z}$, and thus that $x - y \in 8\mathbb{Z}$. Since $8\mathbb{Z} \subseteq 4\mathbb{Z}$, this means that $x - y \in 8\mathbb{Z} \subseteq 4\mathbb{Z}$. This means that $x + 4\mathbb{Z} = y + 4\mathbb{Z}$, which means that $\bar{x} = \bar{y}$, where bar this time means in $\mathbb{Z}/4\mathbb{Z}$. This means that $\varphi(\bar{x}) = \varphi(\bar{y})$. This proves that the homomorphism is well-defined.

Let $\bar{x} \in \mathbb{Z}/4\mathbb{Z}$, where x is either 0, 1, 2, or 3. Then we see that $\bar{x} = x + 4\mathbb{Z}$. Now let $y = x + 8\mathbb{Z} \in \mathbb{Z}/8\mathbb{Z}$. We see that $\varphi(y) = \varphi(x + 8\mathbb{Z}) = x + 4\mathbb{Z} = \bar{x}$. This shows that φ is surjective.

Let $\bar{r} \in \mathbb{Z}/4\mathbb{Z}$, where r is either 0, 1, 2, or 3. We see that the fiber is all the elements of $\mathbb{Z}/8\mathbb{Z}$, that map to $\bar{r}$. That is, all the elements $x + 8\mathbb{Z}$ such that $\varphi(x + 8\mathbb{Z}) = r + 4\mathbb{Z}$, where $x \in \{0, 1, 2, \dots, 8\}$. We see that this equation is only satisfied as $\varphi(r + 8\mathbb{Z}) = \varphi(2r + 8\mathbb{Z}) = r + 4\mathbb{Z}$. That is, the fiber of $\bar{r} \in \mathbb{Z}/4\mathbb{Z}$ are the elements $\bar{r}, \bar{2r} \in \mathbb{Z}/8\mathbb{Z}$. $\square$

Ex 12 Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. Draw the points on a real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points $-1, i$, and $e^{4\pi i/3}$ of H.

Proof. For a picture and description, see the attached paper $\square$

Ex 14 Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

Proof. a) Let $x + \mathbb{Z}$ be an arbitrary element in $\mathbb{Q}/\mathbb{Z}$. We see that $x = y + r$, where $r \in \mathbb{Z}$ and r is the fractional part of x. Thus, $x + \mathbb{Z} = r + y + \mathbb{Z} = r + \mathbb{Z}$. Thus, r is another representative for $x + \mathbb{Z}$. Since $0 \leq r < 1$, this proves the statement.

b) Let $r + \mathbb{Z}$ be an arbitrary element in $\mathbb{Q}/\mathbb{Z}$, where $0 \leq r < 1$ and $r \in \mathbb{Q}$. Since $r \in \mathbb{Q}$ and $0 \leq r < 1$, this means that $r = \frac{p}{q}$ for $p, q \in \mathbb{N}$. We see that $(r + \mathbb{Z})^q = (r + \mathbb{Z}) + (r + \mathbb{Z}) + \cdots = (r + r + r + \dots) + \mathbb{Z} = qr + \mathbb{Z} = q\frac{p}{q} + \mathbb{Z} = p + \mathbb{Z} = \mathbb{Z}$, where $\dots$ indicates "q" times. Thus, every element has a finite order equal to its denominator. Since the denominator can be arbitrarily large, this means the order can be arbitrarily large.

c) We already showed that all elements of $\mathbb{Q}/\mathbb{Z}$ have finite order. Let $r+\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$, where $r \in \mathbb{R}$. If r were rational, then it would be in $\mathbb{Q}/\mathbb{Z}$ and thus have finite order. If r is irrational, then $(r+\mathbb{Z})^n = nr + \mathbb{Z}$ where $n \in \mathbb{N}$. Suppose $nr \in \mathbb{Z}$. This would mean that $r = \frac{k}{n}$ for some $k \in \mathbb{Z}$. This is a contradiction, as r was assumed to be irrational. Thus, $nr \notin \mathbb{Z}$ for all $n \in \mathbb{N}$. This means that $nr + \mathbb{Z} \neq \mathbb{Z}$ for all $n \in \mathbb{N}$, which proves that $|r| = \infty$. Thus, the torsion supgroup of $\mathbb{R}/\mathbb{Z}$ is $\mathbb{Q}/\mathbb{Z}$.

d) We see that the multiplicative roots of unity in $\mathbb{C}^\times$ are simply the elements $e^{2\pi i r}$ where r is rational between 0 and 1. Define $\varphi : \mathbb{Q}/\mathbb{Z} \to$ the roots of unity in $\mathbb{C}^\times$, by $\varphi(r+\mathbb{Z}) = e^{2\pi i r}$. We see that we let $e^{2\pi i r}$ be an arbitrary element of units of unity, that $\varphi(r+\mathbb{Z}) = e^{2\pi i r}$. Thus, φ is surjective. We also see that if $\varphi(x+\mathbb{Z}) = \varphi(y+\mathbb{Z})$, then $e^{2\pi i x} = e^{2\pi i y}$, which are equal if and only if $x = y + n$ for some $n \in Z$. This means that $x - y = n \in \mathbb{Z}$, which means that $x + \mathbb{Z} = y + \mathbb{Z}$. This proves that φ is injective. φ is a homomorphism, as $\varphi(x+\mathbb{Z})\varphi(y+\mathbb{Z}) = e^{2\pi i x}e^{2\pi i y} = e^{2\pi i x + 2\pi i y} = e^{2\pi i(x+y)} = \varphi((x+y)+\mathbb{Z}) = \varphi((x+\mathbb{Z})+(y+\mathbb{Z}))$. This proves that φ is a homomorphism, and thus is also an isomorphism.

$\square$

Ex 17 Let G be the dihedral group of order 16

$$G = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

and let $\bar{G} = G/\langle r^4 \rangle$ be the quotient of G be the subgroup generated by r^4.

a) Show that the order of $\bar{G}$ is 8.

b) Exhibit each element of $\bar{G}$ in the form $\bar{s}^a\bar{r}^b$ for some integers a and b.

c) Find the order of each of the elements of $\bar{G}$ exhibited in (b)

d) Write each of the following elements of $\bar{G}$ in the form $\bar{s}^a\bar{r}^b$, for some integers a and b as in (b): $\overline{rs}, \overline{sr^2s}, \overline{s^{-1}r^{-1}sr}$.

e) Prove that $\bar{H} = \langle \bar{s}, \bar{r}^2 \rangle$ is a normal subgroup of $\bar{G}$ and $\bar{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\bar{H}$ in G.

f) Find the center of $\bar{G}$ and describe the isomorphism type of $\bar{G}/\mathbb{Z}\left(\bar{G}\right)$.

Proof. a) In the last homework, we proved in Sec 1.2 Ex 4, that the element r^4 has order 2. This means, by the additional problems in the last homework that the subgroup generated by r^4 has order 2 as well. This means that $\langle r^4 \rangle = \{1, r^4\}$. By Legrange's Theorem, $\left|\bar{G}\right| = \left|\frac{G}{\langle r^4 \rangle}\right| = \frac{|G|}{|\langle r^4 \rangle|} = \frac{16}{2} = 8$. This proves the statement.

b) Let $s^i r^j$ be in arbitrary element in G where $i \in \{0,1\}$ and $0 \leq j \leq 7$. We see that if $j \geq 4$, then let $b = j - 4$. This gives us $s^i r^j = s^i r^b r^4$. We see that in $\bar{G}$, this elements becomes $s^i r^b r^4 \langle r^4 \rangle = s^i r^b \langle r^4 \rangle$. Thus, the elements of $\bar{G}$ are $\bar{s}^a \bar{r}^b$ where $a \in \{0,1\}$ and $0 \leq b \leq 3$, which gives us all 8 elements in $\bar{G}$.

c) Didn't do the rest.

$\square$

Ex 20 Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\tilde{G} = G/\langle \bar{12} \rangle$, where for each integer a we simplify notation by writing $\tilde{\bar{a}}$ as $\tilde{a}$.

a) Show that $\tilde{G} = \{\tilde{0}, \tilde{1}, \ldots, \tilde{11}\}$.

b) Find the order of each element of $\tilde{G}$

c) Prove that $\tilde{G} \simeq \mathbb{Z}/12\mathbb{Z}$.

Proof. a) We see that $\bar{12} + \bar{12} = \bar{24} = \bar{0}$. Thus, $|\bar{12}| = 2$, which means $|\langle \bar{12} \rangle| = 2$. Since G has 24 elements, by Legrange's Theorem, $\tilde{G}$ has 12 elements. Let $\bar{x} \in \mathbb{Z}/24\mathbb{Z}$. If $\bar{x} > 11$, then let $\bar{y} = \bar{x} - \bar{12}$. We see that in $\tilde{G}$, $\bar{x} + \langle \bar{12} \rangle = \bar{y} + \bar{12} + \langle \bar{12} \rangle = \bar{y} + \langle \bar{12} \rangle$. This means that $\bar{x} + \langle \bar{12} \rangle = \bar{x} - \bar{12} + \langle \bar{12} \rangle$. Thus, the elements $\bar{12}$ and up are redundant to the elements $\bar{0}, \bar{1}, \ldots, \bar{11}$. Since $\tilde{G}$ has 12 elements, these must be the elements of $\tilde{G}$.

b) $\tilde{0}$ is the identity, so it has order 1. Let $\tilde{x} \in \tilde{G}$. Let $|\tilde{x}| = n$. We then see that $|\tilde{x}| = \tilde{x}^n = n\tilde{x} = \tilde{0} = \tilde{12}$. Thus, the order of $\tilde{x} \in \tilde{G}$ is the smallest natural number n where $n\tilde{x}$ is a multiple of 12. We see easily then that $\left|\tilde{1}\right| = 12$, $\left|\tilde{2}\right| = 6$, $\left|\tilde{3}\right| = 4$, $\left|\tilde{4}\right| = 3$, $\left|\tilde{5}\right| = 12$, and that $\left|\tilde{6}\right| = 2$. By the first homework, we proved that the order of an inverse of an element is equal to the order of that element. Thus, for $\tilde{x}$, where $x \geq 6$, there's a $\tilde{y}$ where $y \leq 6$ and $\tilde{x} + \tilde{y} = 12 = 0$, which means $\tilde{x} = -\tilde{y}$. Thus, $|\tilde{x}| = |\tilde{y}|$ for some $y \leq 6$. This gives the orders of all the other elements as duplicates of the original 6.

c) We see that $\tilde{G} = \langle \tilde{1} \rangle$, and that $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle$. Since these groups have the same number of elements, and they're both cyclic groups, this means they must be isomorphic by Thm 4 of section 2.3.

$\square$

Ex 37 Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Proof. Let $g = (a, b) \in A \times B$. And let $H = \{(h, 1) \mid h \in A\}$. We see that $gHg^{-1} = (a, b)(h, 1)(a^{-1}, b^{-1}) = (aha^{-1}, bb^{-1}) = (aha^{-1}, 1) \in H$. This proves that H is normal. Consider the function $\varphi : A \times B \to B$ where $\varphi((a, b)) = b$. We see that $\varphi((a, b)(c, d)) = \varphi((ac, bd)) = bd = \varphi((a, b))\,\varphi((c, d))$. Thus, this is a homomorphism. Let $b \in B$. We see that $\varphi((1, b)) = b$, thus, φ is surjective. We see that $\ker \varphi$ is $\{(a, b) \in A \times B \mid \varphi((a, b)) = b = 1\}$. Thus, $\ker \varphi = \{(a, 1) \in A \times B\} = H$. By the first isomorphism theorem, we see that $(A \times B)/\ker \varphi = (A \times B)/H = \operatorname{Im} \varphi = B$. This proves the statement. $\square$

Ex 41 Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian (N is called the commutator subgroup of G)

Proof. We see that if $x, y, g \in G$ then $gx^{-1}y^{-1}xyg^{-1} = gx^{-1}g^{-1}gy^{-1}g^{-1}gxg^{-1}gyg$. Pairing up by three's we get $(gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1})$. If one lets $a = gxg^{-1}$ and $b = gyg^{-1}$, then this becomes $a^{-1}b^{-1}ab$, which is in N. Thus, we see that $gNg^{-1} = g\langle x^{-1}y^{-1}xy \mid x, y \in G\rangle g^{-1} = \langle gx^{-1}y^{-1}xyg^{-1} \mid x, y \in G\rangle = \langle a^{-1}b^{-1}ab \mid a, b \in G\rangle = N$. Thus, we see that N is normal.

We see that $x^{-1}y^{-1}xy = (yx)^{-1}xy \in N$ for all $x, y \in G$. We see that this means that $xyN = yxN$, which implies that $(xN)(yN) = (yN)(xN)$ for all $x, y \in G$. Thus, G/N is abelian. □

Additional Problems

Ex A Recall that a group G acts on itself by $g.x = gxg^{-1}$. Let X be the set of all subgroups of G. We then have an action on X by $g.H = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. Recall that we've proved already that gHg^{-1} is a subgroup of G whenever H is a subgroup of G. Prove H is normal if and only if H is a fixed point of X under this action.

Proof. Suppose H is a fixed point of X under this action. This means that $g.H = H$ for all $g \in G$. That is, $g.H = gHg^{-1} = H$ for all $g \in G$. This is precisely one of the definitions of a normal subgroup, therefore H is normal.

Suppose H were normal. Then by definition $gHg^{-1} = H$ for all $g \in G$. However, in terms of the above group action, we see that $g.H = gHg^{-1}$. Thus, this means that $g.H = H$ for all $g \in G$. Since for all $g \in G$, $g.H = H$, we see that H is a fixed point for this group action. □

Ex B Recall that D_{2n} acts on the set of edges of the regular polygon with n vertices.

a) Using the Orbit-Stabilizer Lemma, please compute the order of the stabilizer of the edge which connects vertices 1 and 2. Please determine the stabilizer subgroup of this edge. Let's call the stabilizer subgroup of this edge S.

b) Using Legrange's Theorem, please compute the order of D_{2n}/S.

c) Please give a complete list of the elements of D_{2n}/S.

d) Prove that S is not a normal subgroup of D_{2n}. Please give examples of the binary operation on cosets which shows that it is not well-defined.

Proof. a) We see that this edge could go to any other edge. Since there are n edges, there are n elements in the orbit of this particular edge. Thus, by the Orbit-Stabilizer Lemma, the number of stabilizers of this edge is the number of elements in the group divided by the number of elements in the orbit. Since the group has $2n$ elements, and there are n elements in the orbit, there must be 2 elements in the stablizer. These elements are 1 and s where s is the reflection along the line that exchanges vertex 1 with vertex 2. Thus, $S = \{1, s\}$.

b) By Legrange's theorem, we see that $|D_{2n}/S| = \frac{|D_{2n}|}{|S|} = \frac{2n}{2} = n$.

c) Let $s^i r^j$ be an arbitrary element of D_{2n}, where $0 \leq i \leq 1$ and $0 \leq j < n$. We see that if $i = 1$, this $sr^j = r^{-j}s$. This element represents the coset $r^{-j}sS = r^{-j}S$. If $i = 0$, then the element r^j would represent the coset r^jS. These are redundent representations. Thus the lists of D_{2n}/S are the elements r^j where $0 \leq j < n$.

d) We see that $rS = rsS = sr^{-1}S$, which means that rS and $sr^{-1}S$ are the same coset. We also that trivally that $1S$ and sS are the same coset. However, we see that $(1S)(rS) = rS$, while $(sS)(sr^{-1}S) = ssr^{-1}S = r^{-1}S = r^{n-1}S$. These are not the same cosets in general. Thus, S is not a normal subgroup of D_{2n}.

$\square$