Mathematics 243, section 3 – Algebraic Structures
Problem Set 9
due: Friday, November 30

'A' Section

1. For each of the following values of n,
   - Find all distinct generators of the group $(\mathbb{Z}_n, +)$,
   - Find all subgroups of $(\mathbb{Z}_n, +)$ and their orders
   - Find all elements of $(\mathbb{Z}_n^\times, \cdot)$ and their orders (for the *multiplication operation* mod n now)

$$n = 13, 16, 30$$

(Use the "big theorem" on cyclic groups for as much of this as possible. It is not necessary to do a lot of computations in most cases.)

Solution: For $n = 13$, by the "big theorem" we know that the generators of $\mathbb{Z}_{13}$ are the $[a]$ such that $\gcd(a, 13) = 1$, which are $[1], [2], [3], [4], \ldots, [12]$. The only subgroups are $\{[0]\}$ and $\mathbb{Z}_{13}$ itself.

For the multiplication operation, $\mathbb{Z}_{13}^\times = \{[1], [2], \ldots, [13]\}$, and now taking powers $[2]^k$ we get:

$$\langle [2] \rangle = \{[1], [2], [4], [8], [3], [6], [12], [11], [9], [5], [10], [7]\} = \mathbb{Z}_{13}^\times$$

This shows $\mathbb{Z}_{13}^\times$ *is cyclic of order 12* with generator $[2]$. That says that $[1]$ generates the trivial subgroup consisting of just the identity. The elements $[2]^5 = [6]$, $[2]^7 = [11]$, $[2]^{11}$ are the other generators of $\mathbb{Z}_{13}^\times$ and have multiplicative order 12. Then $[2]^2 = [4]$ and $[2]^{10} = [10]$ generate the cyclic subgroup of order 6, so have multiplicative order 6. Also, $[2]^3 = [8]$ and $[2]^9 = [5]$ generate the cyclic subgroup of order 4, so have multiplicative order 4, Next, $[2]^4 = [3]$ and $[2]^8$ generate a cyclic subgroup of order 3 and have multiplicative order 3. Finally, $[2]^6 = [12]$ generates a cyclic subgroup of order 2 and has multiplicative order 2.

$n = 16$: By the "big theorem" we know that the generators of the cyclic group $(\mathbb{Z}_{16}, +)$ are the $[a]$ such that $\gcd(a, 16) = 1$, which are $[1], [3], [5], [7], [9], [11], [13], [15]$. The additive subgroups of $\mathbb{Z}_{16}$ are

$$\begin{aligned} \{[0]\} &= \langle [0] \rangle \\ \mathbb{Z}_{16} &= \langle [1] \rangle = \langle [3] \rangle = \cdots = \langle [15] \rangle \\ \{[0], [2], [4], [6], [8], [10], [12], [14]\} &= \langle [2] \rangle = \langle [6] \rangle = \langle [10] \rangle = \langle [14] \rangle \\ \{[0], [4], [8], [12]\} &= \langle [4] \rangle = \langle [12] \rangle \\ \{[0], [8]\} &= \langle [8] \rangle. \end{aligned}$$

The number of generators in each case is given by the Euler function from Problem Set 7: There are $\varphi(o([a]))$ different generators of the group if the order is $o([a])$.

For the multiplication operation, $\mathbb{Z}_{16}^{\times} = \{[1],[3],[5],[7],[9],[11],[13],[15]\}$. We have the following (finding the smallest positive powers giving the multiplicative identity [1]):

$$\begin{aligned}
o([1]) &= 1\\
o([3]) &= 4 \text{ since } [3]^4 = [81] = [1]\\
o([5]) &= 4 \text{ since } [5]^4 = [625] = [1]\\
o([7]) &= 2 \text{ since } [7]^2 = [49] = [1]\\
o([9]) &= 2 \text{ since } [9]^2 = [81] = [1]\\
o([11]) &= 4 \text{ since } [11]^4 = [1]\\
o([13]) &= 4 \text{ since } [13]^4 = [1]\\
o([15]) &= 2 \text{ since } [15]^2 = [1].
\end{aligned}$$

(Note that this shows $\mathbb{Z}_{16}^{\times}$ is *not a cyclic group* under multiplication.)

$n = 30$: By the "big theorem" we know that the generators of the cyclic group $(\mathbb{Z}_{30}, +)$ are the $[a]$ such that $\gcd(a, 30) = 1$, which are $[1],[7],[11],[13],[17],[19],[23],[29]$. The additive subgroups of $\mathbb{Z}_{30}$ are

$$\begin{aligned}
\{0\} &= \langle[0]\rangle\\
\mathbb{Z}_{30} &= \langle[1]\rangle = \langle[7]\rangle = \cdots = \langle[29]\rangle\\
\{[0],[2],[4],\ldots,[28]\} &= \langle[2]\rangle = \langle[4]\rangle = \langle[8]\rangle = \langle[14]\rangle = \langle[16]\rangle\\
&= \langle[22]\rangle = \langle[26]\rangle = \langle[28]\rangle\\
\{[0],[3],[6],\ldots,[27]\} &= \langle[3]\rangle = \langle[9]\rangle = \langle[21]\rangle = \langle[27]\rangle\\
\{[0],[5],[10],[15],[20],[25]\} &= \langle[5]\rangle = \langle[25]\rangle\\
\{[0],[6],[12],[18],[24]\} &= \langle[6]\rangle = \langle[12]\rangle = \langle[18]\rangle = \langle[24]\rangle\\
\{[0],[10],[20]\} &= \langle[10]\rangle = \langle[20]\rangle\\
\{[0],[15]\} &= \langle[15]\rangle.
\end{aligned}$$

Again, number of generators in each case is given by the Euler function from Problem Set 7: $\varphi(o([a]))$.

For the multiplication operation, $\mathbb{Z}_{30}^{\times} = \{[1],[7],[11],[13],[17],[19],[23],[29]\}$. We find that

$$\begin{aligned}
o([1]) &= 1 \\
o([7]) &= 4 \text{ since } [7]^4 = [1] \\
o([11]) &= 2 \text{ since } [11]^2 = [1] \\
o([13]) &= 4 \text{ since } [13]^4 = [1] \\
o([17]) &= 4 \text{ since } [17]^4 = [1] \\
o([19]) &= 2 \text{ since } [19]^2 = [1] \\
o([23]) &= 4 \text{ since } [23]^4 = [1] \\
o([29]) &= 2 \text{ since } [29]^2 = [1].
\end{aligned}$$

(Note that this shows $\mathbb{Z}_{16}^{\times}$ is *not a cyclic group* under multiplication.)

2. Let $\varphi : \mathbb{Z}_{18} \to \mathbb{Z}_9$ be defined by $\varphi([x]) = [3x]$.

   (a) Verify that φ is a group homomorphism.

   Solution: φ is a group homomorphism since for all $[x]$ and $[y]$ in $\mathbb{Z}_{18}$,

   $$\varphi([x] + [y]) = \varphi([x + y]) = [3(x + y)] = [3x] + [3y] = \varphi([x]) + \varphi([y]).$$

   (b) Determine the kernel of φ.

   Solution: The kernel of φ is

   $$\varphi^{-1}(\{[0]\}) = \{[0], [3], [6], [9], [12], [15]\} = \langle [3] \rangle \subset \mathbb{Z}_{18}$$

   (c) Determine the image of φ.

   Solution: The image of φ is

   $$\varphi(\mathbb{Z}_{18}) = \{[0], [3], [6]\} = \langle [3] \rangle \subset \mathbb{Z}_9$$

'B' Section

1. Let G be a group and consider the mapping $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$. Show that φ is always one-to-one and onto, but that φ is an isomorphism of groups if and only if G is an *abelian* group.

   Solution: The map φ is one-to-one since $\varphi(x) = \varphi(y)$ implies $x^{-1} = y^{-1}$, and taking inverses of both sides we get $x = y$. The map φ is onto because given any $x \in G$, $x = (x^{-1})^{-1} = \varphi(x^{-1})$. This is a group isomorphism if and only if

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

   where the last equality follows from the reverse order law. Since φ is one-to-one, this is equivalent to saying that $x * y = y * x$ for all $x, y \in G$ and hence G is abelian. Hence φ is an isomorphism of groups if and only if G is an abelian group.

2. An *automorphism* of a group G is an isomorphism of groups $\varphi : G \to G$ (that is, the domain and the range are both the same group G).

   (a) Let $A = \{a, b, c\}$ and $G = \mathcal{S}(A)$ be the group of permutations of A. Show that $\varphi : G \to G$ defined by $\varphi(f) = R_a \circ f \circ R_a$ is an automorphism of G.

   Solution: φ is a one-to-one mapping from G to itself since if $\varphi(f) = \varphi(g)$, then $R_a \circ f \circ R_a = R_a \circ g \circ R_a$. Composing with R_a again on the left and right on both sides, since $R_a \circ R_a = I_A$, we get $f = g$. Since $\mathcal{S}(A)$ is a finite set and φ is one-to-one, it is also onto. Finally, φ is an isomorphism of groups since

$$\begin{aligned}\varphi(f \circ g) &= R_a \circ f \circ g \circ R_a \\ &= R_a \circ f \circ R_a \circ R_a \circ g \circ R_a \quad \text{since } R_a \circ R_a = I_A \\ &= (R_a \circ f \circ R_a) \circ (R_a \circ g \circ R_a) \text{ (associativity of composition)} \\ &= \varphi(f) \circ \varphi(g).\end{aligned}$$

   (b) Show that the collection of all automorphisms of a general group G is itself a group under the operation of function composition.

   Solution: We must show that the four axioms (properties) in the definition of a group are satisfied.

   - First, if φ, ψ are automorphisms of G, then $\varphi \circ \psi$ is one-to-one and onto by theorems from Chapter 1. The composition is also an isomorphism of groups since

$$\begin{aligned}(\varphi \circ \psi)(x * y) &= \varphi(\psi(x * y)) \\ &= \varphi(\psi(x) * \psi(y)) \text{ since } \psi \text{ is a homomorphism} \\ &= \varphi(\psi(x)) * \varphi(\psi(y)) \text{ since } \varphi \text{ is a homomorphism} \\ &= (\varphi \circ \psi)(x) * (\varphi \circ \psi)(y).\end{aligned}$$

     Thus the set of automorphisms is closed under composition.
   - Function composition is always associative, so there is nothing more to prove for that property in the definition of a group.
   - The identity map I_G, defined by $I_G(x) = x$ for all $x \in G$, is one-to-one and onto and satisfies

$$I_G(x * y) = x * y = I_G(x) * I_G(y).$$

     Hence it is an isomorphism from G to itself, and it is the identity under composition, since $\varphi \circ I_G = \varphi = I_G \circ \varphi$ for any automorphism φ of G.
   - Finally, if φ is an isomorphism, then the inverse mapping φ^{-1} exists as a mapping from G to itself and is also one-to-one and onto. We want to show that φ^{-1} also has the homomorphism property. So let $x, y \in G$. Since φ is onto, we know $x = \varphi(a)$ and $y = \varphi(b)$ for some unique $a, b \in G$. Therefore since φ is a homomorphism, we have $\varphi(a * b) = x * y$. But this also says $\varphi^{-1}(x) * \varphi^{-1}(y) = a * b = \varphi^{-1}(x * y)$. Hence φ^{-1} is also a group homomorphism.

(c) Show if G is a general group and $g \in G$, then the conjugation mapping defined by $\varphi_g(x) = gxg^{-1}$ is an automorphism of G. (Note that the example in part (a) has this form.)

Solution: φ_g is one-to-one since if $\varphi_g(x) = \varphi_g(y)$, then $gxg^{-1} = gyg^{-1}$. But that implies $g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$, so $x = y$. Next, φ_g is onto since given $y \in G$, $y = \varphi_g(g^{-1}yg) = gg^{-1}ygg^{-1}$. Finally, φ_g is a group homomorphism since for all $x, y \in G$, as in part (a) above

$$\begin{aligned}\varphi_g(xy) &= gxyg^{-1} \\ &= gx(g^{-1}g)yg^{-1}, \text{ since } g^{-1}g = e \\ &= (gxg^{-1})(gyg^{-1}) \text{ by associativity} \\ &= \varphi_g(x)\varphi_g(y).\end{aligned}$$

(d) Show that the collection of φ_g for all $g \in G$ (as in part (c)) is a *subgroup* of the group of automorphisms of G.

Solution: We will use the "shortcut method" from Theorem 3.10. First, this collection of automorphisms is certainly nonempty since we have one of them for each $g \in G$. (They might not be distinct, of course.) Let φ_g and φ_h be any two such automorphisms. Note that φ_h^{-1} is the mapping $\varphi_{h^{-1}}$ since

$$y = \varphi_h(x) = hxh^{-1} \Leftrightarrow x = h^{-1}yh = \varphi_{h^{-1}}(y).$$

Then $\varphi_g \circ \varphi_h^{-1}$ is the mapping defined by

$$(\varphi_g \circ \varphi_h^{-1})(x) = gh^{-1}xhg^{-1} = (gh^{-1})x(gh^{-1})^{-1} = \varphi_{gh^{-1}}(x).$$

This is the automorphism φ_k for $k = gh^{-1} \in G$. Hence this collection of automorphisms is a subgroup of the group of all automorphisms.

3. We can consider isomorphism of groups as a relation on the collection of all groups: $GRH \Leftrightarrow$ there exists an isomorphism $\varphi : G \to H$. Show that isomorphism of groups is an *equivalence relation* on the collection of all groups.

Solution: Every group is isomorphic to itself via the identity mapping $I_G : G \to G$ with $I_G(g) = g$ for all $g \in G$. This is clearly one-to-one, onto, and a group homomorphism. Thus the isomorphism relation is *reflexive*. Next, if G is isomorphic to H via $\varphi : G \to H$, then since φ is one-to-one and onto, we have the inverse mapping $\varphi^{-1} : H \to G$. We want to show that φ^{-1} also has the homomorphism property. So let $x, y \in H$, Since φ is onto, we know $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in G$. Therefore since φ is a homomorphism, we have $\varphi(a * b) = x * y$. But this also says $\varphi^{-1}(x) * \varphi^{-1}(y) = a * b = \varphi^{-1}(x * y)$. Hence φ^{-1} is also a group homomorphism from H to G. Thus φ^{-1} is also an isomorphism of groups. Hence H is isomorphic to G and the isomorphism relation is *symmetric*. Finally, say G is isomorphic to H via $\varphi : G \to H$ and H is isomorphic to K via $\psi : H \to K$. Consider $\psi \circ \varphi : G \to K$.

We know from general results from Chapter 1 that $\psi \circ \varphi$ is one-to-one and onto. Moreover, for all $x, y \in G$,

$$\begin{aligned}(\varphi \circ \psi)(x *_G y) &= \varphi(\psi(x *_G y)) \\ &= \varphi(\psi(x) *_H \psi(y)) \text{ since } \psi \text{ is a homomorphism} \\ &= \varphi(\psi(x)) *_K \varphi(\psi(y)) \text{ since } \varphi \text{ is a homomorphism} \\ &= (\varphi \circ \psi)(x) *_K (\varphi \circ \psi)(y).\end{aligned}$$

Thus $\varphi \circ \psi$ is also an isomorphism from G to K. This shows the isomorphism relation is transitive.

Comment: You should note that the ideas here are the same as those in the proof of part (b) of question 2 above(!)

4. Let $G = \langle a \rangle$ be a cyclic group and let $\varphi : G \to H$ be a group homomorphism. Show that if we know the one element $\varphi(a)$, then we know where φ maps every element of G.

Solution: If $G = \langle a \rangle$ is a cyclic group, then every element of the group G is a^n for $n \in \mathbb{Z}$. If $n = 0$, then $a^0 = e_G$ and $\varphi(e_G) = e_H$. If $n > 0$, then we argue by induction that $\varphi(a^n) = (\varphi(a))^n$ (so knowing $\varphi(a)$ determines all of those elements too). The base case for the induction is $n = 1$, and there is nothing to prove there. Assume we know $\varphi(a^k) = (\varphi(a))^k$. Then

$$\begin{aligned}\varphi(a^{k+1}) &= \varphi(a^k * a) \text{ by definition of the power} \\ &= \varphi(a^k) * \varphi(a) \text{ by the homomorphism property} \\ &= (\varphi(a))^k * \varphi(a) \text{ by the induction hypothesis} \\ &= (\varphi(a))^{k+1} \text{ by the definition of the power.}\end{aligned}$$

This shows $\varphi(a^n) = (\varphi(a))^n$ for all $n \geq 1$. A similar induction also shows $\varphi(a^n) = (\varphi(a))^n$ for all $n \leq -1$. The base case there is the fact we proved in general before: $\varphi(a^{-1}) = (\varphi(a))^{-1}$.