Homework 3 Solutions

Chapter 4

1. Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

$\mathbb{Z}_6$: $\bar{1}$, $\bar{5}$ since $\gcd(1,6) = \gcd(5,6) = 1$

$\mathbb{Z}_8$: $\bar{1}$, $\bar{3}$, $\bar{5}$, $\bar{7}$ (all elements of $U(8)$)

$\mathbb{Z}_{20}$: $\bar{1}$, $\bar{3}$, $\bar{7}$, $\bar{9}$, $\bar{11}$, $\bar{13}$, $\bar{17}$, $\bar{19}$ (all elements of $U(20)$)

2. Suppose $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ are cyclic groups of orders 6, 8, and 20, respectively. Find all generators of $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$.

As in #1, find powers of the generator which are relatively prime to order of the group:

$\langle a\rangle$: a, a^5 $\quad\langle b\rangle$: b, b^3, b^5, b^7 $\quad\langle c\rangle$: c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, c^{19}

7. Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

Consider $G = D_3$. D_3 is not cyclic, but its proper subgroups are all cyclic:

$\langle R_0\rangle = \{R_0\}$, $\langle R_{120}\rangle = \{R_0, R_{120}, R_{240}\}$, $\langle V\rangle = \{R_0, V\}$, $\langle D\rangle = \{R_0, D\}$, $\langle D'\rangle = \{R_0, D'\}$.

8. Let $a \in G$ and $|a| = 15$. Compute the orders of the following elements of G:

(a) $|a^3| = |a^6| = |a^9| = |a^{12}| = \frac{15}{\gcd(15,3)} = \frac{15}{3} = 5$.

(b) $|a^5| = |a^{10}| = \frac{15}{\gcd(15,5)} = \frac{15}{5} = 3$

(c) $|a^2| = |a^4| = |a^8| = |a^{14}| = \frac{15}{\gcd(15,2)} = \frac{15}{1} = 15$

9. How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of them. Suppose $G = \langle a\rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of them.

In both cases, the number of subgroups is the number of positive divisors of 20. The divisors of 20 are 1, 2, 4, 5, 10, and 20, so these groups have $\boxed{6}$ subgroups.

$\mathbb{Z}_{20}$: $\langle \bar{1}\rangle = \mathbb{Z}_{20}$, $\langle \bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \ldots, \bar{18}\}$, $\langle \bar{4}\rangle = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}\}$,

$\langle \bar{5}\rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}\}$, $\langle \bar{10}\rangle = \{\bar{0}, \bar{10}\}$, $\langle \bar{0}\rangle = \{\bar{0}\}$.

G: $G = \langle a\rangle$, other generators are a^2, a^4, a^5, a^{10}, and a^0.

10. In $\mathbb{Z}_{24}$, list all generators for the subgroup of order 8. Let $G = \langle a\rangle$ and $|a| = 24$. List all generators for the subgroup of order 8.

The subgroup of order 8 in $\mathbb{Z}_{24}$ is $\langle \bar{3}\rangle$; the generators are the powers of $\bar{3}$ that are relatively prime to 8: $\bar{3}$, $3\cdot\bar{3} = \bar{9}$, $5\cdot\bar{3} = \bar{15}$, $7\cdot\bar{3} = \bar{21}$. Similarly, the generators for the subgroup $\langle a^3\rangle$ of order 8 in G are a^3, a^9, a^{15}, and a^{21}.

11. Let G be a group and $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.

Proof Since $a^{-1} \in \langle a \rangle$, certainly $\langle a^{-1} \rangle \subseteq \langle a \rangle$. Also, $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$, so $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Thus, $\langle a \rangle = \langle a^{-1} \rangle$. ▨

12. In $\mathbb{Z}$ find all generators of the subgroup $\langle 3 \rangle$. If $a \in G$ has infinite order, find all generators of the subgroup $\langle a^3 \rangle$.

The only generators of $\langle 3 \rangle = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ are 3 and -3.

The only generators of $\langle a^3 \rangle$ in G are a^3 and a^{-3}.

13. In $\mathbb{Z}_{24}$ find a generator for $\langle \overline{21} \rangle \cap \langle \overline{10} \rangle$. Suppose that $a \in G$ and $|a| = 24$. Find a generator for $\langle a^{21} \rangle \cap \langle a^{10} \rangle$. In general, what is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

In $\mathbb{Z}_{24}$, $\langle \overline{21} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\}$, $\langle \overline{10} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}\} \Rightarrow \langle \overline{21} \rangle \cap \langle \overline{10} \rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\} = \langle \overline{6} \rangle$, so a generator is $\overline{6}$.

Similarly, a generator in G for $\langle a^{21} \rangle \cap \langle a^{10} \rangle$ is a^6. In general, a generator for $\langle a^m \rangle \cap \langle a^n \rangle$ is a^l, where $l = \text{lcm}(m, n) \bmod 24$.

21. Let G be a group and $a \in G$.

(a) If $a^{12} = e$, what can we say about $|a|$? We know $|a| \mid 12$, so $|a| \in \{1, 2, 3, 4, 6, 12\}$.

(b) If $a^m = e$, what can we say about $|a|$? That $|a|$ divides m.

(c) Suppose that $|G| = 24$ and G is cyclic. If $\exists\, a \in G$ s.t. $a^8 \neq e$ and $a^{12} \neq e$, then $G = \langle a \rangle$.

Proof [Since $a^8 \neq e$, certainly $a \neq e$.] We know $\langle a \rangle \leq G$, and G is cyclic of order 24, so the only possible orders for a are $1, 2, 3, 4, 6, 8, 12$, and 24 (i.e. the divisors of 24). But $a^8 \neq e$ implies $|a| \nmid 8$, which excludes $1, 2, 4$, and 8. Likewise, $a^{12} \neq e$ implies $|a| \nmid 12$, which excludes $1, 2, 3, 4, 6$, and 12. The only remaining possibility is $|a| = 24$, which implies $G = \langle a \rangle$ since $|G| = 24$. ▨

22. Prove that a group of order 3 must be cyclic.

Proof Let $G = \{e, a, b\}$ be a group of order 3. Since G is closed under multiplication, we have $ab = e$, $ab = a$, or $ab = b$. If $ab = a$ then $b = e$ - contradiction, and if $ab = b$ then $a = e$ - contradiction. So $ab = e$ and $b = a^{-1}$. Again by closure of multiplication, we have $a^2 = e$, $a^2 = a$, or $a^2 = b$. If $a^2 = e$ then $a = a^{-1} = b$ - contradiction, and if $a^2 = a$ then $a = e$ - contradiction. Thus, $a^2 = b$. Then $G = \{e, a, a^2\} = \langle a \rangle$, so G is cyclic. ▨

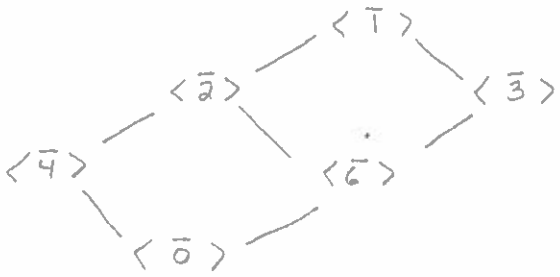
31. Let G be a finite group. Show that $\exists\, n \in \mathbb{Z}^+$ s.t. $a^n = e \;\; \forall a \in G$.

Proof Let $G = \{a_1, \dots, a_r\}$. Since $\langle a_i \rangle \leq G \;\; \forall 1 \leq i \leq r$ and G is finite, we must have $|a_i| < \infty \;\; \forall i$. Let $|a_i| = n_i$. Choose $n = n_1 n_2 \dots n_r$. Then for any $a_i \in G$,

$$a_i^{\,n} = a_i^{\,n_1 n_2 \dots n_r} = (a_i^{\,n_i})^{n/n_i} = e^{n/n_i} = e.$$ Since $n_i \in \mathbb{Z}^+ \;\forall i$, $n \in \mathbb{Z}^+$, so we are done. ▨

32. Determine the subgroup lattice for $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12}$ has six subgroups: $\{\bar{0}\}$, $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$, $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$, $\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$, and $\langle \bar{1} \rangle = \mathbb{Z}_{12}$. The lattice is



40. Let $m, n \in \mathbb{Z}$. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

Any integer in the subgroup $\langle m \rangle \cap \langle n \rangle$ will be a common multiple of m and n. By HW 0.10, a generator for this subgroup is $\underline{\text{lcm}(m,n)}$ since every common multiple of m and n is also a multiple of $\text{lcm}(m,n)$.

54. Suppose that G is a cyclic group + that 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If a is one element of order 8, list the other elements of order 8.

The elements of order 6 will all generate the unique subgroup of order 6 (since G is cyclic $\Rightarrow$ it has one subgroup of order d for every divisor d of $|G|$). Thus, the number of elements of order 6 is $\phi(6) = \boxed{2}$. Similarly, if $8 \mid |G|$, the number of elements of order 8 is $\phi(8) = \boxed{4}$. If a is one element of order 8, the others are a^3, a^5, a^7.

55. List all the elements of $\mathbb{Z}_{40}$ that have order 10. Let $x \in G$ with $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.

The elements of $\mathbb{Z}_{40}$ of order 10 are the generators of the subgroup $\langle \bar{4} \rangle$ of order 10. There are $\phi(10) = 4$ of them: $\bar{4}$, $3 \cdot \bar{4} = \overline{12}$, $7 \cdot \bar{4} = \overline{28}$, and $9 \cdot \bar{4} = \overline{36}$. Similarly, the elements of $\langle x \rangle$ of order 10 are x^4, x^{12}, x^{28}, and x^{36}.

62. Given the fact that $U(49)$ is cyclic and has 42 elements, deduce the number of generators that $U(49)$ has without actually finding any of the generators.

Since $U(49)$ is cyclic and $|U(49)| = 42$, it is generated by elements of order 42. By Theorem 9 the number of such elements is $\phi(42) = \boxed{12}$. $[1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41]$

72. Let $a \in G$ s.t. $|a| = 48$. For each part find a divisor K of 48 satisfying the equation:

(a) $\langle a^{21} \rangle = \langle a^K \rangle$: since $\gcd(21, 48) = 3$, any divisor s.t. $\gcd(K, 48) = 3$ works, including only $K = 3$.

(b) $\langle a^{14} \rangle = \langle a^K \rangle$: since $\gcd(14, 48) = 2$, need $K = 2$

(c) $\langle a^{18} \rangle = \langle a^K \rangle$: since $\gcd(18, 48) = 6$, need $K = 6$.

Chapter 5

1. $\alpha = (12)(45)$, $\beta = (16532)$

(a) $\alpha^{-1} = (21)(54) = \boxed{(12)(45)}$

(b) $\beta\alpha = (16532)(12)(45) = \boxed{(26543)}$

(c) $\alpha\beta = (12)(45)(16532) = \boxed{(16453)}$

2. (a) $\alpha = (12345)(678)$, $\beta = (23847)(56) \Rightarrow \alpha\beta = \boxed{(12485736)}$

(b) $\alpha = (12)(23)(34)(45)(67)(78)$, $\beta = (23)(38)(84)(47)(56)$, $\alpha\beta = (12)(24)(48)(85)(57)(73)(36)$

3. (a) $(1235)(413) \longrightarrow (15)(234)$

(b) $(13256)(23)(46512) \longrightarrow (124)(35)(6)$

(c) $(12)(13)(23)(142) \longrightarrow (1423)$

5. (a) $|(124)(357)| = \text{lcm}(3, 3) = (3)$

(b) $|(124)(3567)| = \text{lcm}(3, 4) = (12)$

(c) $|(124)(35)| = \text{lcm}(2, 3) = (6)$

(d) $|(124)(357869)| = \text{lcm}(3, 6) = (6)$

(e) $|(1235)(24567)| = |(124)(3567)| = \text{lcm}(3, 4) = (12)$

(f) $|(345)(245)| = |(25)(34)| = \text{lcm}(2, 2) = (2)$

7. What is the order of the product of a pair of disjoint cycles of lengths 4 and 6?

$\text{lcm}(4, 6) = (12)$

12. Let S be a finite set and $f: S \to S$ a function. Then f is one-to-one iff f is onto.

Proof Let $S = \{s_1, \ldots, s_n\}$. Suppose first that f is one-to-one and assume by way of contradiction that f is not onto. Then $\exists s_i \in S$ s.t. $f(s_j) \neq s_i \ \ \forall 1 \leq j \leq n$. Since f is a function, each element s_j has an image, but there are at most $n-1$ options since s_i is not the image of any element. Since there are n elements, $\exists k, \ell, m \in \{1, \ldots, n\}$ s.t. $f(s_k) = f(s_\ell) = s_m$ with $s_k \neq s_\ell$. But this contradicts that f is one-to-one, so f must be onto.

Suppose now that f is onto and assume $f(s_i) = f(s_j)$ for some $i, j \in \{1, \ldots, n\}$. If $i \neq j$, there are at most $n-1$ images in S, but since $|S| = n$, there exists an element of S that has no preimage under f. This contradicts the assumption that f was onto, so $i = j$ and thus f is one-to-one. ☒ (Cont'd on next page)

12, cont. This is not true when S is infinite. As a counterexample, consider $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(a) = 2a$. Then f is one-to-one since $f(a) = f(b) \Rightarrow 2a = 2b \Rightarrow a = b$, but f is not onto since there is no integer that gets mapped to $1 \in \mathbb{Z}$.

35. Let G be a group of permutations on a set X and let $a \in X$. Prove that $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$ is a subgroup of G.

Proof Since the identity permutation fixes every element, it certainly fixes a, so it belongs to $\text{stab}(a)$ and $\text{stab}(a)$ is nonempty. If $\alpha \in \text{stab}(a)$, then $\alpha(a) = a \Rightarrow \alpha^{-1}(a) = a$, so we have $\alpha^{-1} \in \text{stab}(a)$ also. If $\alpha, \beta \in \text{stab}(a)$, then $\alpha(a) = a = \beta(a)$. Then $\alpha\beta(a) = \alpha(\beta(a)) = \alpha(a) = a$, so $\alpha\beta \in \text{stab}(a)$. Thus, $\text{stab}(a)$ is a subgroup of G. ▨

40. In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.

Cyclic subgroup: $\langle (1234) \rangle = \{(1), (1234), (13)(24), (1432)\}$

Noncyclic subgroup: $\{(1), (12), (34), (12)(34)\}$. Every nonidentity element has order 2, so the subgroup is not cyclic and is closed under inverses. Closed under products:
$(12)(34) = (12)(34) = (34)(12)$, $(12)(12)(34) = (12)(34)(12) = (34)$, $(34)(12)(34) = (12)(34)(34) = (12)$.

42. In S_3, find elements α, β s.t. $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

Let $\alpha = (12)$, $\beta = (13)$. Then $|\alpha| = 2$, $|\beta| = 2$. Also, $\alpha\beta = (132)$ and $|\alpha\beta| = 3$.

(Other examples are possible.)

76. Given that $\beta, \gamma \in S_4$ with $\beta\gamma = (1432)$, $\gamma\beta = (1243)$, and $\beta(1) = 4$, determine β and γ.

Note $2 = \gamma\beta(1) = \gamma(4)$, $3 = \beta\gamma(4) = \beta(2)$, $4 = \gamma\beta(2) = \gamma(3)$, $2 = \beta\gamma(3) = \beta(4)$, and $3 = \gamma\beta(4) = \gamma(2)$. Since β, γ are permutations, we must have $\beta(3) = 1$, $\gamma(1) = 1$.

Thus, $\beta = (1423)$, $\gamma = (1)(234)$.