Homework 5 Solutions

Chapter 7

3. Let $H = \{0, \pm 3, \pm 6, \pm 9, \dots\}$. Find all the left cosets of H in $\mathbb{Z}$.

$H = 0 + H = 3 + H = 6 + H$, etc.

$1 + H = \{\dots, -5, -2, 1, 4, 7, 10, \dots\} = 4 + H = 7 + H$, etc.

$2 + H = \{\dots, -4, -1, 2, 5, 8, 11, \dots\} = 5 + H = 8 + H$, etc.

5. Let H be as in #3. Decide whether the following cosets of H are the same.

We know that $a + H = b + H$ iff $b - a \in H$.

(a) $11 + H$ and $17 + H$: since $17 - 11 = 6 \in H$, these cosets are the same.

(b) $-1 + H$ and $5 + H$: since $5 - (-1) = 6 \in H$, these cosets are the same.

(c) $7 + H$ and $23 + H$: since $23 - 7 = 16 \notin H$, these cosets are not the same.

7. Find all of the left cosets of $\{\overline{1}, \overline{11}\}$ in $U(30)$.

Recall that $U(30) = \{\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$. Let $H = \{\overline{1}, \overline{11}\}$.

We have $\overline{1}H = \overline{11}H = H$,

$\overline{7}H = \{\overline{7}, \overline{77}\} = \{\overline{7}, \overline{17}\} = \overline{17}H$,

$\overline{13}H = \{\overline{13}, \overline{143}\} = \{\overline{13}, \overline{23}\} = \overline{23}H$,

$\overline{19}H = \{\overline{19}, \overline{209}\} = \{\overline{19}, \overline{29}\} = \overline{29}H$.

8. Suppose that $|a| = 15$. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

Let $H = \langle a^5 \rangle = \{e, a^5, a^{10}\}$. The left cosets of H are

$eH = a^5H = a^{10}H = H$,

$aH = \{a, a^6, a^{11}\} = a^6H = a^{11}H$,

$a^2H = \{a^2, a^7, a^{12}\} = a^7H = a^{12}H$,

$a^3H = \{a^3, a^8, a^{13}\} = a^8H = a^{13}H$,

$a^4H = \{a^4, a^9, a^{14}\} = a^9H = a^{14}H$.

9. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.

Let $H = \langle a^4 \rangle = \{e, a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}, a^{28}, a^2, a^6, a^{10}, a^{14}, a^{18}, a^{22}, a^{26}\}$.

There are 2 left cosets of H in $\langle a \rangle$; one is H and the other is

$aH = \{a, a^3, a^5, a^7, a^9, a^{11}, a^{13}, a^{15}, a^{17}, a^{19}, a^{21}, a^{23}, a^{25}, a^{27}, a^{29}\}$

15. Let G be a group of order 60. What are the possible orders for the subgroups of G?

By Lagrange's Thrm, the possible orders for a subgroup are the divisors of the order of the group. For a group of order 60, the divisors are $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 40\}$.

16. Suppose $K \lneq H$ and $H \lneq G$. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

The possible orders for any subgroup of G are $\{1, 2, 3, 4, 5, 6, 7, 10, 14, 15, 20, 21, 28, 30, 42, 60, 70, 84, 105, 140, 210, 420\}$. Since $|H| < |G|$ and $|H| > 42$, the list narrows to $\{60, 70, 84, 105, 140, 210\}$. Finally, since $K \leq H$ we must also have $42 \mid |H|$ by Lagrange's Thrm, so $|H| \in \boxed{\{84, 210\}}$.

17. Let G be a group with $|G| = pq$ where p and q are prime. Prove that every proper subgroup of G is cyclic.

Proof Let $H \lneq G$ be a proper subgroup of G. By Lagrange's Thrm, $|H| \in \{1, p, q\}$. If $|H| = 1$, then $H = \langle e \rangle$ is cyclic; if $|H| = p$ or $|H| = q$, then H is a group of prime order, hence cyclic by Corollary 5. Thus, H is cyclic. ▨

21. Suppose G is a finite group with $|G| = n$ and $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$. If $g \in G$ and $g^m = e$, prove that $g = e$.

Proof Since $g^m = e$, we know that $|g|$ divides m. By Corollary 3, we also know that $|g|$ divides n. So $|g|$ is a common divisor of m and n, which implies $|g| \leq \gcd(m, n) = 1$. But $|g| \geq 1$ always holds, so in fact $|g| = 1 \Rightarrow g = e$. ▨

22. Suppose $H, K \leq G$. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.

Note that $H \cap K$ is a subgroup of both H and K. Therefore, by Lagrange's Thrm $|H \cap K|$ divides both 12 and 35. Thus, $|H \cap K| \leq \gcd(12, 35) = 1 \Rightarrow |H \cap K| = 1$.

Generalization: If $H, K \leq G$ and $\gcd(|H|, |K|) = 1$, then $|H \cap K| = 1$.

29. Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.

Proof The possible orders for the elements of G are $\{1, 3, 11, 33\}$ by Corollary 3. Suppose BWOC that G has no element of order 3. If G has an element g of order 33, then $|g| = |\langle g \rangle| = 33 = |G| \Rightarrow G = \langle g \rangle$ is cyclic of order 33. Then by the Fund. Thrm of Cyclic Groups, G has a subgroup of order 3 which contains $\phi(3) = 2$ elements of order 3, a contradiction. So G has no element of order 33. Thus, G consists of the identity and 32 elements of order 11. But each subgroup of G of order 11 contains $\phi(11) = 10$ elements of order 11, so the total number of elements of order 11 in G must be a multiple of 10. Since $10 \nmid 32$, this is a final contradiction. Thus, G has an element of order 3. ▨

31. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.

No: suppose BWOC that $|G| = 55$ and G contains exactly 20 elements of order 11. The other possible element orders are $\{1, 5, 55\}$. If G has an element of order 55, then G is cyclic, and by the Fund. Thrm of Cyclic Groups, it contains exactly 1 subgroup of order 11, which has only 10 elements of order 11, contradicting our assumption that G has 20 such elements. So G has no element of order 55, which implies there is 1 element of order 1, 20 elements of order 11, and $55 - 21 = 34$ elements of order 5. But every subgroup of G of order 5 contains $\phi(5) = 4$ elements of order 5, so the number of elements of order 5 in G must be a multiple of 4. Since $4 \nmid 34$, this is a final contradiction. Hence, G cannot have 20 elements of order 11.

33. Let $H, K \leq G$ where G is finite and $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K||K:H|$.

Proof Since $H \subseteq K$ and $H \leq G$, we have $H \leq K$. By Lagrange's Thrm we have

$$|G:H| = \frac{|G|}{|H|} = \frac{|G|}{|K|} \cdot \frac{|K|}{|H|} = |G:K||K:H|. \quad \blacksquare$$

43. Let G be a group of permutations of a set S. Prove that the orbits of the members of S constitute a partition of S.

Proof First, if $s \in S$ then $s \in orb_G(s)$ since certainly $(1) \in G$. Thus every orbit is nonempty. This also shows that $S \subseteq \bigcup_{s \in S} orb_G(s)$. Since $orb_G(s) \subseteq S$ $\forall s \in S$, we also have $\bigcup_{s \in S} orb_G(s) \subseteq S$, so $S = \bigcup_{s \in S} orb_G(s)$. It remains to show that distinct orbits are actually disjoint. Suppose $s, t \in S$ and $x \in orb_G(s) \cap orb_G(t)$. Then $\exists \alpha, \beta \in G$ s.t. $\alpha(s) = x = \beta(t)$. Thus, $\beta^{-1}\alpha(s) = \beta^{-1}(x) = t$. If $y \in orb_G(t)$, then $\exists \gamma \in G$ s.t. $y = \gamma(t) = \gamma(\beta^{-1}\alpha(s))$, so $y \in orb_G(s)$. Thus, $orb_G(t) \subseteq orb_G(s)$. Conversely, $\alpha^{-1}\beta(t) = s$ implies that if $y \in orb_G(s)$, then $\exists \delta \in G$ s.t. $y = \delta(s) = \delta(\alpha^{-1}\beta(t)) \in orb_G(t)$, so $orb_G(s) \subseteq orb_G(t)$. Thus, $orb_G(s) = orb_G(t)$ and the set of orbits forms a partition of S. $\blacksquare$

45. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$

(a) $stab_G(1) = \{(1), (24)(56)\}$, $orb_G(1) = \{1, 2, 3, 4\}$

(b) $stab_G(3) = \{(1), (24)(56)\}$, $orb_G(3) = \{3, 4, 1, 2\}$

(c) $stab_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\}$, $orb_G(5) = \{5, 6\}$

65. If G is a finite group with $|G| < 100$ and G has subgroups of orders 10 and 25, what is $|G|$?

By Lagrange's Thrm, $|G|$ must be a multiple of 10 and 25. We have $\mathrm{lcm}(10, 25) = 50$, so by HW 0.10, $|G|$ is a multiple of 50. But since $|G| < 100$, we must have $|G| = \boxed{50}$.

Chapter 8

2. Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.

Note that every nonidentity element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has order 2 [the elements are $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,0)$, $(1,0,1)$, $(0,1,1)$, $(1,1,1)$], so each of these elements generates a subgroup of order 2, and there are seven of these. Every subgroup of order 2 is generated by an element of order 2, and since the only other element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the identity of order 1, there are no additional subgroups of order 2.

3. Let G be a group with identity e_G and H a group with identity e_H. Prove that $G \cong G \oplus \{e_H\}$ and $H \cong \{e_G\} \oplus H$.

Proof: Define $\phi: G \to G \oplus \{e_H\}$ by $\phi(g) = (g, e_H)$. Let $g_1, g_2 \in G$ and suppose $\phi(g_1) = \phi(g_2)$. Then $(g_1, e_H) = (g_2, e_H) \Rightarrow g_1 = g_2$, so ϕ is injective. If $(g, e_H) \in G \oplus \{e_H\}$, then $\phi(g) = (g, e_H)$, so ϕ is surjective. Let $g_1, g_2 \in G$. Then $\phi(g_1 g_2) = (g_1 g_2, e_H) = (g_1, e_H)\cdot(g_2, e_H) = \phi(g_1)\phi(g_2)$, so ϕ preserves the group operations. Thus, ϕ is an isomorphism.

Define $\psi: H \to \{e_G\} \oplus H$ by $\psi(h) = (e_G, h)$. By symmetry with def. of ϕ, ψ is also an isomorphism. ▨

4. Show that $G \oplus H$ is abelian if and only if G and H are abelian. State the general case.

Proof: Suppose first that $G \oplus H$ is abelian. Let $g_1, g_2 \in G$ and $h_1, h_2 \in H$. Then $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1) \Rightarrow (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) \Rightarrow g_1 g_2 = g_2 g_1$ and $h_1 h_2 = h_2 h_1$. Thus, G and H are abelian.

Conversely, suppose G + H are abelian. Let $g_1, g_2 \in G$, $h_1, h_2 \in H$. Then $g_1 g_2 = g_2 g_1$ and $h_1 h_2 = h_2 h_1$ $\Rightarrow (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) \Rightarrow (g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$. Thus, $G \oplus H$ is abelian. ▨

General case: $G_1 \oplus \dots \oplus G_n$ is abelian if and only if G_i is abelian $\forall i \in \{1, \dots, n\}$.

6. Prove, by comparing orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Note that $(\bar{1}, \bar{0}) \in \mathbb{Z}_8 \oplus \mathbb{Z}_2$ is an element of order 8, but there is no element of order 8 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. If $\bar{a}, \bar{b} \in \mathbb{Z}_4$, then $4\bar{a} = 4\bar{b} = \bar{0}$ by a corollary of Lagrange's Thrm, so $4\cdot(\bar{a}, \bar{b}) = (4\bar{a}, 4\bar{b}) = (\bar{0}, \bar{0})$, which implies $|(\bar{a}, \bar{b})| \leq 4$. Thus, no element of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has order 8, so $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

7. Prove that $G_1 \oplus G_2 \cong G_2 \oplus G_1$. State the general case.

Proof: Let $\phi: G_1 \oplus G_2 \to G_2 \oplus G_1$ be given by $\phi(g_1, g_2) = (g_2, g_1)$ for $g_1 \in G_1$, $g_2 \in G_2$.

Let $g_1, g_1' \in G_1$, $g_2, g_2' \in G_2$ and suppose that $\phi(g_1, g_2) = \phi(g_1', g_2')$. Then $(g_2, g_1) = (g_2', g_1') \Rightarrow g_1 = g_1'$, $g_2 = g_2'$ $\Rightarrow (g_1, g_2) = (g_1', g_2')$. Thus ϕ is injective.

If $(g_2, g_1) \in G_2 \oplus G_1$, then $(g_1, g_2) \in G_1 \oplus G_2$ and $\phi(g_1, g_2) = (g_2, g_1)$, so ϕ is surjective.

Let $g_1, g_1' \in G_1$, $g_2, g_2' \in G_2$. Then $\phi(g_1, g_2)\phi(g_1', g_2') = (g_2, g_1)(g_2', g_1') = (g_2 g_2', g_1 g_1')$ $= \phi(g_1 g_1', g_2 g_2') = \phi((g_1, g_2)(g_1', g_2'))$. Thus ϕ preserves group operations, + ϕ is an isomorphism. ▨

General case: $G_1 \oplus \dots \oplus G_n \cong G_{\sigma(1)} \oplus \dots \oplus G_{\sigma(n)}$ for any $\sigma \in S_n$

8. Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{27}$? Why?

No. Corollary 2 to Thrm 8.2 states that $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $\gcd(m,n)=1$. Since $\gcd(3,9)=3 \neq 1$, we cannot have $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{27}$.

9. Is $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}$? Why?

Yes, by the Corollary referenced in #8, $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{3\cdot 5} = \mathbb{Z}_{15}$ since $\gcd(3,5)=1$.

10. How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have?

Let $(\bar{a},\bar{b}) \in \mathbb{Z}_3 \oplus \mathbb{Z}_9$. We know $|(\bar{a},\bar{b})| = 9$ if $\operatorname{lcm}(|\bar{a}|,|\bar{b}|)=9$. Now $|\bar{a}| \in \{1,3\}$ and $|\bar{b}| \in \{1,3,9\}$ by Lagrange's Thrm. So $|(\bar{a},\bar{b})|=9 \Rightarrow |\bar{b}|=9 \Rightarrow \bar{b}$ generates $\mathbb{Z}_9$. Recall that $\mathbb{Z}_9$ has $\phi(9)=6$ generators. There is no restriction on $\bar{a} \in \mathbb{Z}_3$, so there are $3\cdot 6 = 18$ elements of order 9 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$.

16. Suppose that $G_1 \cong G_2$ and $H_1 \cong H_2$. Prove that $G_1 \oplus H_1 \cong G_2 \oplus H_2$ and state the general case.

Proof Since $G_1 \cong G_2$, there is an isomorphism $\phi: G_1 \to G_2$; since $H_1 \cong H_2$, there is an isomorphism $\psi: H_1 \to H_2$. Define $\alpha: G_1 \oplus H_1 \to G_2 \oplus H_2$ by $\alpha(g,h) = (\phi(g), \psi(h))$ for $g \in G_1$, $h \in H_1$. Let $g_1, g_2 \in G_1$, $h_1, h_2 \in H_1$ and suppose that $\alpha(g_1,h_1) = \alpha(g_2,h_2)$. Then $(\phi(g_1),\psi(h_1)) = (\phi(g_2),\psi(h_2)) \Rightarrow \phi(g_1)=\phi(g_2)$ and $\psi(h_1)=\psi(h_2)$. Since ϕ and ψ are injective, this implies $g_1 = g_2$, $h_1 = h_2 \Rightarrow (g_1,h_1) = (g_2,h_2)$. Thus, α is injective. Let $g_2 \in G_2$, $h_2 \in H_2$. Since ϕ is surjective, $\exists g_1 \in G_1$ s.t. $\phi(g_1) = g_2$; similarly, $\exists h_1 \in H_1$ s.t. $\psi(h_1) = h_2$. Then $(g_1,h_1) \in G_1 \oplus H_1$ and $\alpha(g_1,h_1) = (\phi(g_1),\psi(h_1)) = (g_2,h_2) \in G_2 \oplus H_2$, so α is onto. Finally, let $g, g' \in G_1$ and $h, h' \in H_1$. Then since ϕ, ψ are operation-preserving, we have

$$\alpha((g,h)(g',h')) = \alpha(gg',hh') = (\phi(gg'),\psi(hh')) = (\phi(g)\phi(g'),\psi(h)\psi(h'))$$
$$= (\phi(g),\psi(h))(\phi(g'),\psi(h')) = \alpha(g,h)\alpha(g',h'),$$

so α is also operation-preserving. Thus, α is an isomorphism. ☒

General case: If $G_1 \cong H_1, \ldots, G_n \cong H_n$, then $G_1 \oplus \cdots \oplus G_n \cong H_1 \oplus \cdots \oplus H_n$.

7. If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.

Proof Assume that $G \oplus H$ is cyclic. Now $|G \oplus H| = |G|\cdot|H|$ is divisible by $|G|$, so by the Fund. Thrm of Cyclic Groups, there is a unique subgroup of $G \oplus H$ of order $|G|$, and it is cyclic. We know $G \oplus \{e_H\} \leq G \oplus H$ and $|G \oplus \{e_H\}| = |G|$, so it must be this unique subgroup. Therefore, $G \oplus \{e_H\}$ is cyclic. Then by #3, $G \oplus \{e_H\} \cong G$, so G is also cyclic. Replacing G with H and $G \oplus \{e_H\}$ with $\{e_G\} \oplus H$ in this argument yields that H is cyclic. ☒

General case: If $G_1 \oplus \cdots \oplus G_n$ is cyclic, then G_i is cyclic $\forall i \in \{1,\ldots,n\}$.

8. In $\mathbb{Z}_{40} \oplus \mathbb{Z}_{30}$, find two subgroups of order 12.

Since $2\cdot 6 = 12$ with $2|40$ and $6|30$, find a subgroup of $\mathbb{Z}_{40}$ of order 2 and a subgroup of $\mathbb{Z}_{30}$ of order 6 and take their external direct product: $H = \langle \overline{20} \rangle \oplus \langle \bar{5} \rangle$.

Similarly, $4\cdot 3 = 12$ with $4|40$ and $3|30$, so $K = \langle \overline{10} \rangle \oplus \langle \overline{10} \rangle$.

20. Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ that is isomorphic to $\mathbb{Z}_9 \oplus \mathbb{Z}_4$.

Want a subgroup of $\mathbb{Z}_{12}$ of order 4 and a subgroup of $\mathbb{Z}_{18}$ of order 9. So we have $\langle \bar{3} \rangle \oplus \langle \bar{2} \rangle \leq \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ and $\langle \bar{3} \rangle \oplus \langle \bar{2} \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_9 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{36}$ since $\gcd(4,9) = 1$.

21. Let G and H be finite groups and $(g,h) \in G \oplus H$. State a necessary and sufficient condition for $\langle (g,h) \rangle = \langle g \rangle \oplus \langle h \rangle$.

Since we always have $\langle (g,h) \rangle \subseteq \langle g \rangle \oplus \langle h \rangle$, we need a condition for $|\langle g \rangle \oplus \langle h \rangle| = |\langle (g,h) \rangle|$. We have $|\langle (g,h) \rangle| = |(g,h)| = \operatorname{lcm}(|g|, |h|)$ and $|\langle g \rangle \oplus \langle h \rangle| = |g| \cdot |h|$. Then $\operatorname{lcm}(|g|,|h|) = |g| \cdot |h|$ if and only if $\gcd(|g|, |h|) = 1$.

22. Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$.

Want $(\bar{a}, \bar{b}) \in \mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$ s.t. $\operatorname{lcm}(|\bar{a}|, |\bar{b}|) = 15$. Then we must have $|\bar{a}| = 3, |\bar{b}| = 5$; $|\bar{a}| = 15, |\bar{b}| = 5$; or $|\bar{a}| = 15, |\bar{b}| = 1$. There are $\phi(3) = 2$ elements of order 3 in $\mathbb{Z}_{30}$ and $\phi(5) = 4$ elements of order 5 in $\mathbb{Z}_{20}$, so the first case yields $2 \cdot 4 = 8$ elements.* There are $\phi(15) = 8$ elements of order 15 in $\mathbb{Z}_{30}$ and only 1 element of order 1 in $\mathbb{Z}_{20}$ (the identity), so the third case yields $8 \cdot 1 = 8$ elements. Thus, there are 48 elements of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$.

Since each cyclic subgroup of order 15 contains $\phi(15) = 8$ elements of order 15, and all such elements must lie in only one cyclic subgroup, there are $\frac{48}{8} = 6$ cyclic subgroups of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$.

23. What is the order of any nonidentity element of $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$? Generalize.

Let $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $(\bar{a}, \bar{b}, \bar{c}) \neq (\bar{0}, \bar{0}, \bar{0})$. By a Corollary to Lagrange's Thrm, $3\bar{a} = 3\bar{b} = 3\bar{c} = \bar{0}$, so $|\bar{a}| \in \{1,3\}$, $|\bar{b}| \in \{1,3\}$, $|\bar{c}| \in \{1,3\}$. Since $|(\bar{a}, \bar{b}, \bar{c})| = \operatorname{lcm}(|\bar{a}|, |\bar{b}|, |\bar{c}|) \neq 1$, we must have $|\bar{j}| = 3$ for some $j \in \{a,b,c\}$. Thus, $|(\bar{a}, \bar{b}, \bar{c})| = \operatorname{lcm}(|\bar{a}|, |\bar{b}|, |\bar{c}|) = 3$.

Generalization: The order of any nonidentity element of $\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p$, where p is a prime, is p.

17. Let G be a group and $H = \{(g,g) \mid g \in G\}$. Show that $H \leq G \oplus G$. When $G = (\mathbb{R}, +)$, describe $G \oplus G$ and H geometrically.

Proof Since $e_G \in G$, $(e_G, e_G) \in H$, so H is nonempty. Let $g, h \in G$ and $(g,g), (h,h) \in H$. Then $(g,g)(h,h) = (gh, gh) \in H$ since $gh \in G$. Finally, let $g \in G$ and $(g,g) \in H$. Then $(g,g)^{-1} = (g^{-1}, g^{-1}) \in H$ since $g^{-1} \in G$. Thus, $H \leq G \oplus G$. ∎

When $G = (\mathbb{R}, +)$, $G \oplus G$ is the Cartesian plane and H is the line $y = x$.

---

* There are $\phi(15) = 8$ elements of order 15 in $\mathbb{Z}_{30}$ and $\phi(5) = 4$ elements of order 5 in $\mathbb{Z}_{20}$, so the second case yields $8 \cdot 4 = 32$ elements.

28. Find a subgroup of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ that is <u>not</u> of the form $H \oplus K$, where $H \leq \mathbb{Z}_4$ and $K \leq \mathbb{Z}_2$.

Consider the subgroup $\langle (\bar{1}, \bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{1},\bar{1}), (\bar{2},\bar{0}), (\bar{3},\bar{1})\}$. If it had the form $H \oplus K$, then $H = \{\bar{0},\bar{1},\bar{2},\bar{3}\} = \mathbb{Z}_4$ and $K = \{\bar{0},\bar{1}\} = \mathbb{Z}_2$; but certainly $\langle (\bar{1},\bar{1}) \rangle \neq \mathbb{Z}_4 \oplus \mathbb{Z}_2$ since $|\langle(\bar{1},\bar{1})\rangle| = 4 \neq 8 = |\mathbb{Z}_4 \oplus \mathbb{Z}_2|$.

52. Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$?

We have
$$\begin{aligned}\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 &\cong (\mathbb{Z}_2 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_6 \\ &\cong \mathbb{Z}_2 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_6 \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \text{ (by \#7), so } \underline{\text{yes}}.\end{aligned}$$

53. Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$?

As in #52,
$$\begin{aligned}\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 &\cong (\mathbb{Z}_2 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \\ &\cong (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}_4 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3); \text{ (by \#7)} \\ &\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3) \not\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}\end{aligned}$$
since $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$. So <u>no</u>.