November 4, 2024

Problem Set 7 Solutions

Exercise 1. (a) Let G_1, G_2 be two groups. Show that the group $G_1 \times G_2$ is abelian if and only if both G_1 and G_2 are abelian.

(b) If G_1 and G_2 are both cyclic groups, find the conditions for $G_1 \times G_2$ to be cyclic.

Solution 1. (a) $\Leftarrow$ Suppose G_1 and G_2 are abelian then for every $(a,b),(c,d) \in G_1 \times G_2$ we have that $(a,b)(c,d) = (ac,bd) = (ca,db) = (c,d)(a,b)$. Therefore $G_1 \times G_2$ is abelian. $\Rightarrow$ Suppose $G_1 \times G_2$ is abelian. Then for every $a, c \in G_1$ and $(ac,e) = (a,e)(c,e) = (c,e)(a,e) = (ca,e)$. Therefore $ac = ca$ in G_1. Similarly, one shows that G_2 is abelian. Therefore, G_1 and G_2 are abelian.

(b) Let $G_1 = C_n$ and $G_2 = C_m$, cyclic groups of orders n and m. Then $C_n \times C_m$ is cyclic (of order mn) if and only if $\gcd(n,m) = 1$.
Indeed, let $a \in C_n$ and $b \in C_m$ be elements of orders k and l respectively. Then $(a,b)^t = (a^t, b^t) = (1,1)$ if and only if $k|t$ and $l|t$. Therefore, the order of $(a,b) \in C_n \times C_m$ is $\mathrm{lcm}(k,l)$. Since $k|n$ and $l|m$, the order of the element is maximal if $k = n$ and $l = m$, and in this case the order of (a,b) is $\mathrm{lcm}(n,m)$. We have $\mathrm{lcm}(n,m) = nm$ if and only if $\gcd(n,m) = 1$. Therefore, $C_n \times C_m$ contains an element of order nm if and only if n and m are coprime.

Exercise 2. We proved in class that in any abelian group G such that its order $|G|$ is divisible by a prime p, there exists an element of order p. Use this to prove the same statement for non-abelian groups. As a conclusion, we obtain Cauchy's theorem: any group G such that $|G|$ is divisible by a prime p, contains an element of order p.

Solution 2. Let $Z \subset G$ be the center of the group. If p divides $|Z|$, then Z contains an element of order p by the statement proven in class, since Z is an abelian subgroup. If not, then according to the class equation

$$|G| = |Z| + \sum_{i=1}^{m} |C_i| = |Z| + \sum_{i=1}^{m} [G : G_i],$$

there is at least one nontrivial conjugacy class, say C_j, of order that is not divisible by p. By the orbit-stabilizer theorem we have then $|C_j| = [G : G_i] = |G|/|G_i|$, where $G_j \subset G$ is the centralizer subgroup of the conjugacy class C_j. Since $|C_j|$ is not divisible by p we have that $|G_i|$ is divisible by p, and is a proper subgroup of G. We have $1 < |G_j| < |G|$, and we can finish the proof by induction on the order of G.

Exercise 3. In each case provide the list of elementary divisors and invariant factors for each group.

(a) List all abelian groups of order 8 (up to an isomorphism).

(b) List all abelian groups of order 120 (up to an isomorphism).

Solution 3. (a) By the Theorem of classification of finite abelian groups, we need to consider the prime factorization of the order. We have $8 = 2^3$. Unisomorphic finite abelian groups of order 8 are in $1-1$ correspondence with the partitions of 3: $3, \{1,2\}, \{1,1,1\}$. We obtain the following list:

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2.$$

The elementary divisors are

$$\{8\}, \{4,2\}, \{2,2,2\}.$$

The list of invariant factors is the same in this case.

(b) Using the same theorem, we obtain $120 = 2^3 \cdot 3 \cdot 5$. We have the following list of finite abelian groups of order 120 (up to an isomorphism):

$$C_5 \times C_3 \times C_8, \quad C_5 \times C_3 \times C_4 \times C_2, \quad C_5 \times C_3 \times C_2 \times C_2 \times C_2.$$

The elementary divisors are

$$\{5,3,8\ \}, \{5,3,4,2\}, \{5,3,2,2,2\}.$$

This list can be rewritten using the invariant factors instead of prime powers. These are the integers $d_1, d_2, \dots d_k$ such that $n = d_1 d_2 \dots d_k$ and $d_k | d_{k-1} | \dots | d_2 | d_1$. We have that any abelian group of order 120 is isomorphic to one of the following:

$$C_{120}, \quad C_{60} \times C_2, \quad C_{30} \times C_2 \times C_2.$$

The invariant factors are

$$\{120\}, \{60, 2\}, \{30, 2, 2\}.$$

Exercise 4. (a) Find all abelian groups of order 180 up to an isomorphism and for each group list the elementary divisors (the prime powers in the decomposition of an abelian group as a product of cyclic p-groups) and the invariant factors (the integers $d_1, d_2, \dots d_k$ such that $d_k | d_{k-1} | \dots | d_2 | d_1$ and $d_1 d_2 \dots d_k$ equals the order of the group).

(b) Find the prime power divisors and invariant factors for the group $C_3 \times C_{15} \times C_{20}$.

(c) Are the groups $G_1 = C_{16} \times C_{12} \times C_5$ and $G_2 = C_{10} \times C_{24} \times C_4$ isomorphic?

Solution 4. (a) We have $180 = 2^2 \cdot 3^2 \cdot 5$. By the fundamental theorem of finite abelian groups if G is a finite abelian group of order 180, then G is isomorphic to one of the following 4 groups:

$$C_5 \times C_9 \times C_4, \quad C_5 \times C_9 \times C_2 \times C_2, \quad C_5 \times C_3 \times C_3 \times C_4, \quad C_5 \times C_3 \times C_3 \times C_2 \times C_2.$$

Then elementary divisors are:

$$\{5, 9, 4\}, \{5, 9, 2, 2\}, \{5, 3, 3, 4\}, \{5, 3, 3, 2, 2\}.$$

The invariant factors are obtained by multiplying the highest powers of each prime in the list:

$$\{180\}, \{90, 2\}, \{60, 3\}, \{30, 6\}.$$

(b) We have

$$C_3 \times C_{15} \times C_{20} \simeq C_3 \times C_3 \times C_5 \times C_5 \times C_4 \simeq C_{60} \times C_{15}.$$

So the elementary divisors are $\{5, 5, 3, 3, 4\}$, and the invariant factors are $\{60, 15\}$.

(c) We decompose both groups into a direct product of prime power cyclic groups (cyclic groups corresponding to the elementary divisors):

$$G_1 = C_{16} \times C_{12} \times C_5 \simeq C_{16} \times C_3 \times C_4 \times C_5.$$

$$G_2 = C_{10} \times C_{24} \times C_4 \simeq C_2 \times C_5 \times C_8 \times C_3 \times C_4.$$

The elementary divisors of the two groups are different: $\{5, 3, 16, 4\}$ and $\{5, 3, 8, 4, 2\}$. Therefore by the Theorem of classification of finite abelian groups, they are non-isomorphic. We can also note that G_1 contains an element of order 16, and G_2 does not. Using the invariant factors, we can write: $G_1 \simeq C_{240} \times C_4$, and $G_2 \simeq C_{120} \times C_4 \times C_2$.

Exercise 5. Let $G = (\mathbb{Z}/315\mathbb{Z})^*$, the group of units in $\mathbb{Z}/315\mathbb{Z}$ with respect to the multiplication.

(a) Find the order of G. *Hint:* You can use the multiplicative property of the Euler's totient function: $\varphi(mn) = \varphi(m)\varphi(n)$ if $\gcd(m, n) = 1$.

(b) Show that for all $x \in G$, we have $x^{288} = 1$.

(c) Show that for all $m \in \mathbb{Z}$ such that $(m, 630) = 1$, we have $m^{144} \equiv 1 \pmod{315}$.

(d) Find all solutions modulo 315 of the equation $x^{25} = 1$. (Hint: Note that such x is invertible, and therefore an element in $(\mathbb{Z}/315\mathbb{Z})^*$.

Solution 5. (a) We have $315 = 5 \cdot 7 \cdot 3^2$. The order of the group G is 144 and is given by the Euler's totient function: $\varphi(315) = (5-1) \cdot (7-1) \cdot (9-3) = 144$.

(b) By Lagrange's theorem the order of each element in G has to divide the order of G. In our case the order of each element $x \in G$ divides 144. Therefore for every $x \in G$ we have that $x^{144} = 1$, and also $(x^{144})^2 = 1$.

(c) Observe that $(m, 630) = 1$ implies that $(m, 315) = 1$. Therefore by Euler's Theorem one has that $m^{144} \equiv 1 \pmod{315}$.

(d) Note that a solution x has to belong to $(\mathbb{Z}/315\mathbb{Z})^*$. Now, observe that since $x^{25} = 1$ the order of x has to divide 25. But x belongs to $(\mathbb{Z}/315\mathbb{Z})^*$, therefore its order has to divide also 144. Hence the only solution is $x = 1$.

Exercise 6. Use Lagrange's theorem to classify all groups of order 6 up to isomorphism. Let $|G| = 6$.

(a) Consider possible orders of elements in G. Consider the case when G contains an element of order 6.

(b) Show that G cannot contain only elements of order 1 and 2.

(c) Show that G cannot contain only elements of order 1 and 3.

(d) Identify the group of 6 elements that contains elements of order 1, 2 and 3, and does not contain an element of order 6.

Solution 6. (a) By a corollary of Lagrange's theorem, the order of elements of G divide the order of G. Therefore, we can only have elements of order 1, 2, 3 and 6 in G. If $g \in G$ has order 6, then G contains the set of elements $\{1, g, g^2, g^3, g^4, g^5\} \subset G$, where all the elements are distinct (if $g^i = g^k$, then $g^{i-k} = 1$ which is only possible if 6 divides $i - k$). Therefore, in this case G is isomorphic to a cyclic group C_6.

(b) Suppose G contains only elements of order 1 and 2. The only element of order 1 is the identity. If $a, b \in G$ are two elements of order 2, then $ab \in G$ and we suppose that ab is also of order 2. Then $abab = 1$ and we have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. But then $\{1, a, b, ab\} \subset G$ is a subgroup of G, which is impossible because by Lagrange's theorem the order of a subgroup divides the order of the group.
Also, by Cauchy's theorem (Ex. 2 PS7) if a prime 3 divides $|G|$, then G contains an element of order 3.

(c) Suppose G contains only elements of order 1 and 3. If $a \in G$ is an element of order 3, then G also contains its inverse $a^{-1} = a^2$. Similarly, any element of order 3 and its inverse form a subset of two elements in G, so G contains several pairs of elements and the identity. Then the number of elements in G is odd, which is impossible.
Also, by Cauchy's theorem (Ex. 2 PS7) if a prime 2 divides $|G|$, then G contains an element of order 2.

(d) We have shown that G must contain an element of order 2 and an element of order 3. Denote them as $a \in G$, $a^3 = 1$ and $b \in G$, $b^2 = 1$. Then the subgroup they generate in G must contain the elements $\{1, a, a^2, b, ba, ba^2\}$. It also has to contain ab. Since there are already 6 elements listed, ab is equal to one of them. Clearly, $ab \neq a$, $ab \neq a^2$ and $ab \neq b$ which leads to $b = 1$, $a = 1$ or $a = b$. If $ab = ba$, then the subgroup generated by a and b in G is abelian, and in this case the order of ab is 6, the product of the coprime orders of a and b (see Exercise 3(c), PS3), which means G is cyclic of order 6. Finally, if $ab = ba^2 = ba^{-1}$, then we see that a, b generate a group isomorphic to the dihedral group D_3:

$$G = \langle a, b \,|\, a^3 = 1, b^2 = 1, bab = a^{-1} \rangle.$$

Finally, there are 2 groups of order 6 up to isomorphism: the cyclic group C_6 and the dihedral group D_3.