Math 120 Homework 6 Solutions

May 22, 2008

p. 156

11.) Every non-identity element of E_{p^n} has order p, hence is contained in a subgroup of order p. Two distinct subgroups of order p intersect at the identity, since the order of their intersection must divide p. Hence every non-identity element is contained in exactly one subgroup of order p. Thus the number of subgroups of order p is $(p^n-1)/(p-1)$ since there are p^n-1 non-identity elements, $p-1$ of which appear in each subgroup.

18.) a. Let $G = \prod_{i=1}^{\infty} Z_2$. This group consists of all sequences of elements $(a_1, a_2, ...)$ with $a_i \in Z_2$. Since there are infinitely many such strings, $|G| = \infty$. Moreover $(a_1, a_2, ...) + (a_1, a_2, ...) = (a_1 + a_1, a_2 + a_2, ...) = (0, 0, ...)$ so for all $a = (a_1, a_2, ...) \in G$, $a + a = 0$. Thus the order of every element of G divides 2 and hence is 1 or 2.

b. Let $G = \mathbb{Q}/\mathbb{Z}$ under addition. Let $\overline{q} = \frac{a}{b} \in G$, $a, b \in \mathbb{Z}$. Then $b\overline{q} = \overline{a} = \overline{0}$ so all elements of G have finite order. Take $\overline{q} = \frac{1}{n}$. Then $q, 2q, ..., (n-1)q \notin \mathbb{Z}$ and $nq \in \mathbb{Z}$ so $\overline{q}$ has order n. Thus G has elements of every finite order. But then it must have infinitely many elements.

c. Let $G = \mathbb{Z} \times Z_2$. Then the element $(1, 0)$ has infinite order since $n(1, 0) = (n, 0) \neq (0, 0)$ while $(0, 1)$ has order 2, since $(0, 1) \neq (0, 0)$ but $(0, 1) + (0, 1) = (0, 2) = (0, 0)$.

d. Let $G = Perm(\mathbb{N}) = Perm(\{1, 2, ...\})$, the set of bijections $\mathbb{N} \to \mathbb{N}$. Then for each n, G contains as a subgroup the collection of permutations fixing $n+1, n+2, ...$, and this subgroup is isomorphic to S_n. Now any finite group is isomorphic to a subgroup of S_k for some k, hence is isomorphic to a subgroup of a subgroup of G, hence is isomorphic to a subgroup of G.

e. Let $G = \mathbb{Q}_+^{\times}$, the positive rational numbers under multiplication. A proof that this is isomorphic to $G \times G$ is given in additional problem number 5. Alternatively, take $G = \prod_{i=1}^{\infty} H$ for any group H.

Additional problems:

1.) By the Fundamental Theorem of Finitely Generated Abelian Groups, the isomorphism type of the group is determined by its primary decomposition. We have $8100 = 2^2 3^3 5^2$. The two partitions of 2 are 2 and $1, 1$. The three partitions of 3 are 3, $2, 1$ and $1, 1, 1$. Hence there are two choices each for the elementary divisors corresponding to $p = 2$ and $p = 5$ and there are three choices for the elementary divisors corresponding to $p = 3$. This gives $2 \times 3 \times 2 = 12$ possible primary decompositions.

2.) a. From the primary decomposition, we have $G \cong Z_{p^2} \times Z_q$ or $G \cong Z_p \times Z_p \times Z_q$. The first group is cyclic since the element $(1,1)$ has order p^2q. Hence we must have $G \cong Z_p \times Z_p \times Z_q$. Now an element of G has form (a_1, a_2, a_3) with $a_1, a_2 \in Z_p$ and $a_3 \in Z_q$. It follows that $pq(a_1, a_2, a_3) = (q(pa_1), q(pa_2), p(qa_3)) = (0,0,0)$ and hence the order of all elements of G divides pq. Now $p(1,1,1) = (p,p,p) = (0,0,p) \neq (0,0,0)$ since $p \neq 0$ in Z_q. Similarly, $q(1,1,1) = (q,q,q) = (q,q,0) \neq (0,0,0)$ since $q \neq 0$ in Z_q. It follows that the order of $(1,1,1)$ divides pq but is not either p or q. Since $(1,1,1)$ is not the identity, it must have order pq and this proves that pq is the maximum order.

b. The elements of G have order dividing pq, hence equal to $1, p, q$ or pq. There is one (identity) element of order 1. Suppose (a_1, a_2, a_3) has order p. Then $(pa_1, pa_2, pa_3) = (0,0,0)$. Now p is invertible in $Z_q^\times$ so $pa_3 = 0$ implies $a_3 = 0$. Moreover $pa_1 = pa_2 = 0$ for any choice of $a_1, a_2 \in Z_p$. Hence all elements of form $(a_1, a_2, 0)$ have order dividing p, and these are the only elements having order dividing p. Since the only factors of p are 1 and p, all elements of form $(a_1, a_2, 0)$ have order p except for the identity. It follows that there are $p^2 - 1$ elements of order p.

Suppose $q(a_1, a_2, a_3) = (qa_1, qa_2, qa_3) = 0$. Then $a_1 = a_2 = 0$ since q is invertible in $Z_p^\times$. Since $qa_3 = 0$ for all choices of a_3, the elements having order dividing q are exactly of form $(0,0,a_3)$. Of these, only the identity does not have order q. Hence we obtain $q-1$ elements of order q.

All remaining elements have order pq, that is, there are $p^2q - (p^2-1) - (q-1) - 1 = p^2q - p^2 - q + 1$ elements of order p^2q.

3.) Suppose for contradiction that $\sigma^3 = (1\ 2\ 3)$. Then $\sigma^9 = (1\ 2\ 3)^3 = id$ and $\sigma, \sigma^3 \neq id$ so $|\sigma| = 9$. This is only possible if the cycle decomposition of σ contains a 9-cycle, since all cycles in the decomposition have length dividing 9 and if σ was composed of 3-cycles it would have order 3. Say $(a_1\ a_2\ \ldots\ a_9)$ is contained in the cycle decomposition of σ. Now disjoint cycles commute, and so $(a_1\ a_2\ \ldots\ a_9)^3 = (a_1\ a_4\ a_7)(a_2\ a_5\ a_8)(a_3\ a_6\ a_9)$ is contained in the cycle decomposition of σ^3. But this contradicts the fact that σ^3 contains a single 3-cycle. Thus there does not exist σ with $\sigma^3 = (1\ 2\ 3)$.

4.) Suppose for contradiction that $\phi : A \times B \to \mathbb{Q}$ is an isomorphism with A, B non-trivial groups. Let $\pi_1 : A \to A \times B$, $\pi_2 : B \to A \times B$ be the inclusion maps: $\pi_1(a) = (a,0)$, $\pi_2(b) = (0,b)$. The maps π_1 and π_2 are injective group homorphisms. It follows that the maps $\phi_1 = \phi \circ \pi_1$ and $\phi_2 = \phi \circ \pi_2$ are injective maps $A \to \mathbb{Q}$ and $B \to \mathbb{Q}$ respectively. Thus the subgroups $\phi_1(A)$ and $\phi_2(B)$ of $\mathbb{Q}$ satisfy $A \cong \phi_1(A)$ and $B \cong \phi_2(B)$ and in particular are non-trivial. So take $\frac{p}{q} \in \phi_1(A)$, $\frac{p'}{q'} \in \phi_2(B)$ with $p, p', q, q' \in \mathbb{Z} \backslash \{0\}$. Then $p'q'\frac{p}{q} = pp' \in \phi_1(A)$ and $pq\frac{p'}{q'} = pp' \in \phi_2(B)$ implies $pp' \in \phi_1(A) \cap \phi_2(B)$ so $pp' = \phi_1(a) = \phi_2(b)$ for some $a \in A$,

$b \in B$. Hence by definitions, $pp' = \phi(a, 0) = \phi(0, b)$. Since ϕ is injective, $a = b = 0$. But then $\phi(0, 0) = pp' \neq 0$ is a contradiction. It follows that it is impossible to write $\mathbb{Q}$ as the direct product of two non-trivial groups.

5.) We prove part b since this implies part a, the group $\mathbb{Q}_+^\times$ being non-trivial. Let $p_1 = 2, p_2 = 3, \ldots$ be an enumeration of the primes. Unique prime factorization implies that each positive rational number q has unique expression

$$q = \prod_{i=1}^{\infty} p_i^{e_i}$$

where each exponent $e_i \in \mathbb{Z}$ and where all but a finite number of the e_i are 0. Define map $\phi : \mathbb{Q}_+^\times \to \mathbb{Q}_+^\times \times \mathbb{Q}_+^\times$ by

$$\phi\left(\prod_{i=1}^{\infty} p_i^{e_i}\right) = \left(\prod_{i=1}^{\infty} p_i^{e_{2i-1}}, \prod_{i=1}^{\infty} p_i^{e_{2i}}\right).$$

We'll show that this is a group isomorphism. Take $q_1 = \prod_{i=1}^{\infty} p_i^{e_i}, q_2 = \prod_{i=1}^{\infty} p_i^{f_i}$. Then

$$\phi(q_1 q_2) = \phi\left(\prod_{i=1}^{\infty} p_i^{e_i+f_i}\right) = \left(\prod_{i=1}^{\infty} p_i^{e_{2i-1}+f_{2i-1}}, \prod_{i=1}^{\infty} p_i^{e_{2i}+f_{2i}}\right)$$

$$= \left(\prod_{i=1}^{\infty} p_i^{e_{2i-1}}, \prod_{i=1}^{\infty} p_i^{e_{2i}}\right)\left(\prod_{i=1}^{\infty} p_i^{f_{2i-1}}, \prod_{i=1}^{\infty} p_i^{f_{2i}}\right) = \phi(q_1)\phi(q_2).$$

This proves that ϕ is a group homomorphism. To prove that ϕ is a bijection, define map $\psi : \mathbb{Q}_+^\times \times \mathbb{Q}_+^\times \to \mathbb{Q}_+^\times$ by

$$\psi\left(\prod_{i=1}^{\infty} p_i^{e_i}, \prod_{i=1}^{\infty} p_i^{f_i}\right) = \prod_{i=1}^{\infty} p_{2i-1}^{e_i} p_{2i}^{f_i}.$$

Then for $q = \prod_{i=1}^{\infty} p_i^{e_i}$,

$$\psi \circ \phi(q) = \psi\left(\prod_{i=1}^{\infty} p_i^{e_{2i-1}}, \prod_{i=1}^{\infty} p_i^{e_{2i}}\right) = \prod_{i=1}^{\infty} p_{2i-1}^{e_{2i-1}} p_{2i}^{e_{2i}} = q.$$

This proves that ϕ is injective. Meanwhile, for $(q_1, q_2) \in \mathbb{Q}_+^\times \times \mathbb{Q}_+^\times$, $q_1 = \prod_{i=1}^{\infty} p_i^{e_i}$ and $q_2 = \prod_{i=1}^{\infty} p_i^{f_i}$ then

$$\phi \circ \psi(q_1, q_2) = \phi\left(\prod_{i=1}^{\infty} p_{2i-1}^{e_i} p_{2i}^{f_i}\right) = \left(\prod_{i=1}^{\infty} p_i^{e_i}, \prod_{i=1}^{\infty} p_i^{f_i}\right) = (q_1, q_2).$$

This proves that ϕ is surjective, hence an isomorphism.