Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 1
January 21, 2008

Section 8.2

1. Let G be an abelian group. By definition, $G(p) = \{a \in G : p^\ell \cdot a = 0 \text{ for some } \ell \geq 0\}$. Let $a, b \in G(p)$. Then $p^\ell \cdot a = 0$ and $p^m \cdot b = 0$ for some $\ell, m \geq 0$. Let $n = \max\{\ell, m\}$. Then $p^n \cdot a = p^n \cdot b = 0$ so

$$p^n \cdot (a - b) = p^n \cdot a - p^n \cdot b = 0 - 0 = 0.$$

This shows that $a - b \in G(p)$. Hence $G(p)$ is a subgroup of G.

2. Let G be an abelian group and let $pG = \{p \cdot x : x \in G\}$. Let $a = p \cdot x$ and $b = p \cdot y$ be elements of pG, where $x, y \in G$. Then $a - b = p \cdot x - p \cdot y = p \cdot (x - y)$ and $x - y \in G$ since G is a group under $+$. Hence $a - b \in pG$, so pG is a subgroup.

3. (d) We have $72 = 2^3 \cdot 3^2$. As in the example on p. 256 in Hungerford or the examples done in class last Friday, the structure theorem implies every abelian group of order 72 has elementary divisors $2^3, 3^2$ or $2^3, 3, 3$, or $2^2, 2, 3^2$, or $2^2, 2, 3, 3$, or $2, 2, 2, 3^2$, or $2, 2, 2, 3, 3$. The group is isomorphic to one of

$$\begin{aligned} \mathbb{Z}_8 \oplus \mathbb{Z}_9, &\qquad \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, &\qquad \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, \quad \text{or} &\qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{aligned}$$

(h) Similarly, $1160 = 2^3 \cdot 5 \cdot 29$, so every abelian group of order 1160 is isomorphic to one of

$$\mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29},\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29},\ \text{or } \mathbb{Z}_2 \oplus Z_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29}.$$

5 (b) We can use the fact that if $(m, n) = 1$, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$ (Lemma 8.8). Applying this,

$$\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18} \simeq (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_9).$$

Since the elementary divisors are unique, this shows the elementary divisors of $\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ are $2, 2, 4, 3, 3, 9$ (reordering to put powers in increasing order).

Comment: Note that this also gives the invariant factors of this group, which is isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{36}$.

8. By definition,

$$G(2) = \left\{ \left[\frac{m}{n}\right] \in \mathbb{Q}/\mathbb{Z} : 2^\ell \cdot \left[\frac{m}{n}\right] = [0] \text{ for some } \ell \geq 0 \right\}.$$

This is equivalent to saying that $2^\ell \frac{m}{n}$ is an integer. If $\frac{m}{n}$ is written in lowest terms, then $n = 2^\ell$ for some $\ell \geq 0$, and hence $G(2)$ is the set of cosets of rational numbers of the form $\frac{m}{2^\ell}$ in lowest terms. Similarly, $G(p)$ is the set of cosets of rational numbers of the form $\frac{m}{p^\ell}$ in lowest terms.

9. (a) Saying G is a p-group means by definition that every element of G has order p^ℓ for some $\ell \geq 0$. If G is also a finite group, then there is some element $m \in G$ of *maximal* order p^{ℓ_0} where $\ell_0 \geq 1$. Now consider the group pG as in Exercise 2 above. If x has order p^ℓ with $\ell \geq 1$, then $p^{\ell-1} \cdot (p \cdot x) = p^\ell \cdot x = 0$, but $p^k \cdot (p \cdot x) = p^{k+1} \cdot x \neq 0$ if $k < \ell - 1$. Hence the order of $p \cdot x$ is $\ell - 1$. This shows that pG cannot contain any elements of order ℓ_0. Hence $pG \neq G$.

(b) Let $G = \mathbb{Q}/\mathbb{Z}$ as in Exercise 8. $G(2)$ is the subgroup consisting of cosets of rational numbers of the form $\frac{m}{2^\ell}$ for all $\ell \geq 0$. Note that $G(2)$ is not a finite group because ℓ can be arbitrarily large. And moreover, if $x = \left[\frac{m}{2^\ell}\right] \in G(2)$ then $x = 2 \cdot \left[\frac{m}{2^{\ell+1}}\right]$ and $y = \left[\frac{m}{2^{\ell+1}}\right] \in G(2)$. This shows that $G(2) \subseteq 2 \cdot G(2)$. The other inclusion is clear, so in fact $G(2) = 2 \cdot G(2)$.

11. By the structure theorem (Theorem 8.7), G is isomorphic to a direct sum of subgroups, each of order q^e for some primes q and exponents $e \geq 1$. If G is a p-group, then only powers of one prime can appear among the elementary divisors, and

$$G \simeq \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_s}} \tag{1}$$

for some $e_i \geq 1$. What we must show is that if $pG = \{0\}$, then all the $e_i = 1$. Assume not. That is, suppose $e_i \geq 2$ for some i. Then let a be a generator of $Z_{p^{e_i}}$, so $|a| = p^{e_i} > p$. In the direct sum we have the element $x = (0, \ldots, 0, a, 0, \ldots, 0)$ (a in the ith factor). Then $p \cdot x = (0, \ldots, 0, p \cdot a, 0, \ldots, 0) \neq (0, \ldots, 0)$. Hence the group $pG \neq \{0\}$. By contraposition, if $pG = \{0\}$, then all $e_i = 1$ in Eq. (1).

12. Let G be a finite abelian group and let $p \mid |G|$. By the structure theorem (Theorem 8.7), G is isomorphic to a direct sum of cyclic groups of prime power orders. Each of those orders must divide $|G|$ and hence at least one must be a power of p (since otherwise the order of G would be a product of powers of primes different from p and that would contradict $p \mid |G|$). Hence

$$G \simeq \mathbb{Z}_{p^k} \oplus H_2 \oplus \cdots \oplus H_s,$$

for some $k \geq 1$ and some cyclic groups $H_2, \ldots, H_s$ of prime power orders. Hence G contains a subgroup isomorphic to $\mathbb{Z}_{p^k}$ for some $k \geq 1$. Let a be a generator of this subgroup, so $|a| = p^k$. By the same sort of argument used in Exercise 9 (a) above, we have $|p^{k-1} \cdot a| = p$ (also see part (4) of Theorem 7.8). Hence G contains an element of order p.

14. We are given that

$$|G| = p^t m \qquad \text{where } (p, m) = 1. \tag{2}$$

By Theorem 8.5, we also have $G \simeq G(p) \oplus H$ where H is the direct sum of the $G(q)$ for the primes $q \neq p$ dividing $|G|$, which implies $|G| = |G(p)| \cdot |H|$. By Lemma 8.6, it follows that $|G(p)| = p^s$ for some s and $|H|$ is a product of powers of primes $q \neq p$. Hence

$$|G| = p^s m' \qquad \text{where } (p, m') = 1. \tag{3}$$

By unique factorization in $\mathbb{Z}$, comparing Eq. (2) and Eq. (3), we see that $t = s$, and $m = m'$. Therefore, $|G(p)| = p^t$ which is what we wanted to show.

15. If $|G| = p^t m$ with $(p, m) = 1$, then Exercise 14 shows that G contains the subgroup $G(p)$ of order p^t. In other words, the statement to be proved is true for $n = t$, the *largest* power of p dividing $|G|$. The statement is also clearly true with $n = 0$, since $\{0\}$ is a subgroup of G.

What remains to be proved is that the same statement is true for all n with $1 \leq n < t$ as well. It suffices to show that $G(p)$ contains a subgroup of order p^n since a subgroup of $G(p)$ is also a subgroup of G. We know

$$G(p) \simeq \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_s}}$$

for some $e_i \geq 1$ satisfying $e_1 + \cdots + e_s = t$. The cyclic group $\mathbb{Z}_{p^e}$ contains elements of orders $1, p, p^2, \ldots, p^e$ since if a is a generator with order p^e, then $p^{e-j} \cdot a$ has order p^j whenever $0 \leq j \leq e$. Now, if $1 \leq n < t$, then we can always write $n = f_1 + \cdots + f_s$ where $0 \leq f_i \leq e_i$ for all i. (In fact, we always can do this in many different ways when $s > 1$). If a_i is a generator of $\mathbb{Z}_{p^{e_i}}$, then that summand contains a subgroup $K_i = \langle p^{e_i - f_i} \cdot a_i \rangle$ of order p^{f_i} by the observation above. Hence $G(p)$ contains the subgroup $K = K_1 \oplus \cdots \oplus K_s$ which has order $p^{f_1 + \cdots + f_s} = p^n$.

16. We claim that this is equivalent to saying that $n = p_1 p_2 \cdots p_s$ for some *distinct* primes $p_1, \ldots, p_s$. Such integers are called *square-free* numbers. If n has this form, then there is just one possibility for the elementary divisors of G, namely the set $p_1, p_2, \ldots, p_s$. By Lemma 8.8 (applied repeatedly), we have

$$G \simeq \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_s} \simeq \mathbb{Z}_{p_1 \cdots p_s} = \mathbb{Z}_n,$$

and there is just one abelian group of order n up to isomorphism. Conversely, suppose there is just one abelian group of order n up to isomorphism. If any prime p satisfies $p^2 \mid |G|$, then there are at least two different possibilities for the elementary divisors of G and hence there are at least two nonisomorphic abelian groups of order n. Hence for each prime p that divides $|G|$, we must have $p^2 \nmid |G|$. Hence n is square-free.