Section 2.13 Exercises
Herstein's Topics In Algebra

Spencer T. Parkin

March 29, 2016

Lemma 1

Let $\{a_i\}_{i=1}^n$ be a set of n elements taken from an abelian group G such that

$$\gcd(a_1, \ldots, a_n) = 1,$$

which is also to say that they, collectively, are coprime. We then have

$$\left| \prod_{i=1}^{n} a_i \right| = \operatorname{lcm}(|a_1|, \ldots, |a_n|).$$

Proof. We begin by observing that

$$\left(\prod_{i=1}^{n} a_i \right)^k = \prod_{i=1}^{n} a_i^k,$$

since G is abelian. That the order of the product is the above least common multiple now follows by the definition of the order of an element. □

Problem 5

Let G be a finite abelian group. Prove that G is isomorphic to the direct preoduct of its Sylow subgroups.

Let's first observe that for every prime divisor p of $|G|$ that there is one and only one p-Sylow subgroup of G. In light of Theorem 2.12.2, this is

because G is abelian, and therefore, every such subgroup is conjugate only with itself.

That said, if $\{P_i\}_{i=1}^n$ denotes the set of all Sylow subgroups of G, then no prime is repeated in the associated set of primes $\{p_i\}_{i=1}^n$. Here, each subgroup P_i is a p_i-Sylow subgroup of G. Now consider the internal direct product

$$\prod_{i=1}^{n} P_i = \left\{ \prod_{i=1}^{n} g_i \middle| \, g_i \in P_i \right\}.$$

The number of products generating this set is clearly

$$\prod_{i=1}^{n} |P_i|,$$

but it remains to be seen whether this is the size of the set. To see that it is, consider the possibility that any two different product are equal to one another. That is, consider the equation

$$\prod_{i=1}^{n} g_i = \prod_{i=1}^{n} g_i'.$$

Rearranging this, we get, for any $1 \leq j \leq n$,

$$g_j (g_j')^{-1} = \prod_{i=1, i \neq j}^{n} g_i (g_i')^{-1}.$$

Now notice that $|g_j (g_j')^{-1}| = p_j^{\alpha_j}$. We then see, by Lemma 1, that the order of the right-hand side our equation is

$$\operatorname{lcm}(p_1^{\alpha_1}, \ldots, p_{j-1}^{\alpha_{j-1}}, p_{j+1}^{\alpha_{j+1}}, \ldots, p_n^{\alpha_n}) = \prod_{i=1, i \neq j}^{n} p_i^{\alpha_i},$$

yet the order of the left-hand side is $p_j^{\alpha_j}$. We must, therefore, concede that $g_j (g_j')^{-1} = e$. It then follows that, for all $1 \leq j \leq n$, we have $g_j = g_j'$, showing that product given earlier is indeed the size of the internal product.

We have now shown that the internal product generates G, and that every elemetn of G has a unique decomposition in terms of one element taken from each Sylow subgroup. We can now apply Theorem 2.13.1 to get the final, desired result.

Problem 6

Let A, B be cyclic groups of order m and n, respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.

Suppose m and n are coprime. Let $a \in A$ and $b \in B$ such that $|a| = m$ and $|b| = n$. Then

$$|(a, b)| = \text{lcm}(m, n) = \frac{mn}{\gcd(m, n)} = mn,$$

showing that $A \times B$ is cyclic.

Conversly, suppose $A \times B$ is cyclic. Let $(a, b) \in A \times B$ such that $|(a, b)| = mn$. Then

$$mn = |(a, b)| = \text{lcm}(m, n) \implies \gcd(m, n) = 1.$$

Problem 7

Use the result of Problem 6 to prove the Chinese Remainder Theorem; namely, if m and n are relatively prime integers and u, v any two integers, then we can find an integer x such that $x \equiv u \mod m$ and $x \equiv v \mod n$.

Without loss of generality, we need only consider any $u \in \mathbb{Z}_m$ and any $v \in \mathbb{Z}_n$. Now by Problem 6, since $\gcd(m, n) = 1$, we have that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic; in fact, $(1, 1)$ is a generator, and it is clear that, for any $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_n = \langle (1, 1) \rangle$, there must exist an integer $x \in \mathbb{Z}$ such that

$$(1, 1)^x = (u, v).$$

Translated, this means that $x \equiv u \pmod m$ and $x \equiv v \pmod n$, as desired.

Problem 15

Let $G = A \times A$ where A is cyclic or order p, p a prime. How many automorphisms does G have?

Let's stop to think about $\text{Aut}(\mathbb{Z}_n)$. As I recall, this group is isomorphic to $U(n)$, and so the number of automorphisms of $\mathbb{Z}_n$ is $\phi(n)$, the Euler totient function. So, the number of automprhisms of A is $p - 1$.

Now what about $A \times A$? It is apparent to me that every non-identity element of this group is of order p. And, admittedly, without giving proof,

(and so I may be wrong), I believe that there exists, for every pair of non-identity elements $(a_1, a_2), (a_3, a_4) \in A \times A$, an automorphism of the group that sends (a_1, a_2) to (a_3, a_4). Doing so, however, we do not entirely determine the automorphism. We, of course, must send the identity element to the identity element, but in sending (a_1, a_2) to (a_3, a_4), we determine only $p - 1$ of the remaining $p^2 - 1$ elements to be mapped. In choosing the next mapping, I believe we, again, can map any of the remaining $p^2 - 1 - (p - 1)$ non-identity elements to any other of such elements not yet mapped in the forming image of the homomorphism. All in all, by the multiplication rule of combinatorics, we arrive at

$$|\mathrm{Aut}(A \times A)| = \prod_{k=0}^{p} (p^2 - 1 - k(p-1))^2$$

as the number of automorphisms of $A \times A$. There, however, is definitely some rigor lacking here. We can be sure that the mapping is one-to-one and onto, but is it operation preserving? I don't think there's any reason to suppose it's not, because the structure is the same everywhere. That's the best I can come up with for now.