

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

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

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

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

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. \square

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

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

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

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

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 element 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.

Conversely, 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 $x \equiv u \pmod{m}$ and $x \equiv v \pmod{n}$.

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 11

Let G be a finite abelian group such that it contains a subgroup $H_0 \neq \{e\}$ which lies in *every* subgroup $H \neq \{e\}$. Prove that G must be cyclic. What can you say about $|G|$?

Suppose p and q are distinct primes, and each a divisor of $|G|$. Then by Theorem 2.11.3, G must have an element of order p , and that of q . Call these a and b , respectively. Now clearly $\langle a \rangle$ and $\langle b \rangle$ are each subgroups of G , but they only have the identity element in common. Being contrary to

hypothesis, we can conclude that G must have one and only one prime divisor of its order; call it p .

Hmmm...so close.

Problem 15

Let $G = A \times A$ where A is cyclic of 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 automorphisms 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 . We can, therefore, begin to construct any automorphism of $A \times A$ by sending any non-identity element to another other (or itself), so long as by the end, we have an operation-preserving bijection of the group. Clearly the identity must go to the identity. This leaves us $p^2 - 1$ elements to map. Then, mapping the first non-identity element actually determines the next $p - 1$ mappings, since each element has order p . This leaves us $p^2 - 1 - (p - 1)$ non-identity elements. Mapping one of these elements to another such, we determine another $p - 1$ mapping, but we actually determine more. Note that if $a, b \in A \times A$ are distinct elements, then $\langle a \rangle \cap \langle b \rangle = \{(e, e)\}$, and $A \times A$ is isomorphic to the inner direct product of $\langle a \rangle$ and $\langle b \rangle$. This causes us to know, for each pair of integers $i, j \in [1, p]$, how our automorphism should map $\phi(a^i b^j) = \phi(a^i) \phi(b^j)$, and so we eat up $(p - 1)^2$ more mappings. But now notice that

$$p^2 - 1 - (p - 1) - (p - 1) - (p - 1)^2 = 0,$$

so we've now completely determined the automorphism. How many ways could we have constructed it? I believe it is

$$(p^2 - 1)^2 (p^2 - 1 - (p - 1))^2 = [p(p^2 - 1)(p - 1)]^2.$$