Chapter 11 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 28, 2014

Understanding the last part of Lemma 1

We have $p^n m = |HK| = |H||K|$ with $\gcd(p^n, m) = 1$. If p divides $|K|$, then K has an element of order p by Theorem 9.5; call it k. But $k \in K \implies k^m = e \implies |k| = p|m$ by Corollary 2 of Theorem 4.1. But this is a contradiction, since $\gcd(p, m) = 1$, and therefore p does not divide $|K|$. Now suppose that $m = qr$ with q prime and that q divides $|H|$. Then H has an element of order q; call it h. But $h \in H \implies h^{p^n} = e \implies |h| = q|p^n$, but $\gcd(q, p) = 1$, so by contradiction, q does not divide $|H|$.

We can now argue that no prime in the factorization p^n appears in $|K|$ and that no prime in the factorization of m appears in $|H|$. So $|H| = p^n$ and $|K| = m$.

Exercise 11

Prove that every finite Abelian group can be expressed as the (external) direct product of cyclic groups of orders $n_1, n_2, \ldots, n_t$, where n_{i+1} divides n_i for $i = 1, 2, \ldots, t-1$.

It is clear by the Fundamental Theorem of Finite Abelian Groups that such a group G can, for some k integers m_1 through m_k, always be written as

$$G = Z_{m_1} \oplus \cdots \oplus Z_{m_k}.$$

We now describe an algorithm for achieving the desired arrangement. First, sort the product so that for any two distinct integers $i, j \in [1, k]$ with $i < j$, we have $m_i \geq m_j$. If we then have the property that for each such pair of integers, $m_j | m_i$, we're done. Otherwise, find any two distinct integers $i, j \in [1, k]$ where $|Z_{m_i}|$ and $|Z_{m_j}|$ are coprime and collapse them into a single group in the product as $Z_{m_i m_j}$. This does not change the group represented, up to isomorphism, by Corollary 2 of Theorem 8.2. Now reduce the integer k by one and go back to the first step with a new set of k integers m_1 through m_k.

What would remain to be shown here is that this algorithm is correct, which is to say that it will always terminate. So suppose we have a group G where this algorithm doesn't terminate. Then we can always find a pair of integers $i, j \in [1, k]$ such that m_i and m_j are coprime, and therefore, we can continue to collapse the product indefinitely. But this is only possible if the $|G| = \infty$, which is a contradiction, because $|G|$ is finite. So the algorithm will always terminate. (This proof is not quite right to me, but it's good enough for now.)

Exercise 20

Suppose that G is a finite Abelian group that has exactly one subgroup for each divisor of $|G|$. Show that G is cyclic.

By the Fundamental Theorem of Finite Abelian Groups, we may write G as

$$G = Z_{n_1} \oplus \cdots \oplus Z_{n_k},$$

for a set of k integers n_1 through n_k. Suppose there exist distinct integers $i, j \in [1, k]$ such that $d = \gcd(n_i, n_j) \neq 1$. It follows that Z_{n_i} and Z_{n_j} each have an element of order d by the Fundamental Theorem of Cyclic Groups; call them z_i and z_j, respectively. We then see that G has two distinct elements of order d, (a divisor of $|G|$ by Lagrange's Theorem), namely, $(e_1, \ldots, a_i, \ldots, e_k)$ and $(e_1, \ldots, a_j, \ldots, e_k)$, that each generate their own distinct subgroups of G of order d. But this violates the premise of the group G, so we can conclude that no such integers i and j exist. It now follows by Corollary 1 of Theorem 8.2 that G is cyclic.

Exercise 21

Characterize those integers n such that the only Abelian groups of order n are cyclic.

Let $n = p_1^{n_1} \dots p_k^{n_k}$ be the prime factorization of n where the primes p_i are distinct. If for each i, we have $n_i = 1$, then we can be assured that Abelian groups of order n are cyclic. If there is any i, such that $n_i > 1$, then there is an Abelian group of order n that is non-cyclic, because there is an Abelian group of order $p_i^{n_i}$ that is non-cyclic.

Exercise 31

Without using Legrange's Theorem, show that an Abelian group of odd order cannot have an element of even order.

By the Fundamental Theorem of Finite Abelian Groups, G has the form $Z_{n_1} \oplus \cdots \oplus Z_{n_k}$ for k integers n_1 through n_k. It follows that $|G| = |n_1| \dots |n_k|$. Suppose now that there exists an integer $i \in [1, k]$ such that n_i is even. It would then follow that $|G|$ is even, which is a contradiction. Therefore, each n_i is odd. It now follows by the Corllary of the Fundamental Theorem of Cyclic Groups (Theorem 4.3), that for no integer i does Z_i have an element of even order. Considering now an element $(a_1, \dots, a_k) \in G$, it is clear by Theorem 8.1, that it does not have even order, because $\operatorname{lcm}(|a_1|, \dots, |a_k|)$ cannot be even.