Chapter 8 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 21, 2014

Understanding Theorem 8.3

We want to show that $U(st) \approx U(s) \oplus U(t)$. Let $\phi(x) = (x \bmod s, x \bmod t)$. For $x, y \in U(st)$, if $\phi(x) = \phi(y)$, then $x \equiv y \pmod{s}$ and $x \equiv y \pmod{t}$. Then, since $\gcd(s,t) = 1$, it is clear that $x \equiv y \pmod{st}$. (See Problem 15 of Chapter 0.) So ϕ is one-to-one. It is also onto since ϕ is onto-to-one and maps a finite set to another of the same cardinality. That ϕ is operation preserving is a matter of showing that for any $x, y \in U(st)$, we have

$$\begin{aligned}(xy \bmod st) \bmod m &= (x \bmod m)(y \bmod m) \bmod st \\ &= (xy \bmod m) \bmod st,\end{aligned}$$

where m is s or t. With enough thought, this is intuitive enough to warrent justification by virtue of being clear.

Problem 1

Prove that the external direct product of any finite number of groups is a group.

There is clearly an identity element. Closure is clear. Inverses are clear. Associativity is clear. I think that's it.

Problem 2

Show that $Z_2 \oplus Z_2 \oplus Z_2$ has seven subgroups of order 2.

Considering $\langle(a,b,c)\rangle$ for any $(a,b,c) \in Z_2 \oplus Z_2 \oplus Z_2$ for which not all of a, b and c are zero, it is clear that there are $2^3 - 1 = 7$ such cases. Are there any more subgroups of order 2? Hmmm...

Problem 4

Show that $G \oplus H$ is Abelian if and only if G and H are Abelian.

If G and H are Abelian, then for any $(g_0, h_0), (g_1, h_1) \in G \oplus H$, we have

$$(g_0, h_0)(g_1, h_1) = (g_0 g_1, h_0 h_1) = (g_1 g_0, h_1 h_0) = (g_1, h_1)(g_0, h_0),$$

showing that $G \oplus H$ is Abelian too. If $G \oplus H$ is Abelian, then for any $a, b \in G$, and $e_H \in H$, we have

$$(ab, e_H) = (a, e_H)(b, e_H) = (b, e_H)(a, e_H) = (ba, e_H),$$

which implies that $ab = ba$, showing that G is Abelian. A similar argument shows that H is Abelian.

Problem 5

Prove or disprove that $Z \oplus Z$ is a cyclic group.

Supping $Z \oplus Z$ to be cyclic, there exists $(a, b) \in Z \oplus Z$ such that $Z \oplus Z = \langle(a, b)\rangle$. Clearly $a \neq 0$ and $b \neq 0$. Now if $(x, y) \in Z \oplus Z$, then so is $(x+1, y)$, and there exist integers $z_0, z_1 \in Z$ such that

$$\begin{aligned}(x, y) &= (z_0 a, z_0 b),\\ (x+1, y) &= (z_1 a, z_1 b).\end{aligned}$$

It follows that $z_0 b = z_1 b \implies z_0 = z_1$, and then that $z_0 a + 1 = z_1 a \implies a(z_0 - z_1) = 1 \implies 0 = 1$, which is a contradiction. The group $Z \oplus Z$ is therefore not cyclic.

Problem 6

Prove, by comparing orders of elements, that $Z_8 \oplus Z_2$ is not isomorphic to $Z_4 \oplus Z_4$.

Notice that $Z_8 \oplus Z_2$ has an element of order 8, but $Z_4 \oplus Z_4$ does not.

Problem 18

Let $m > 2$ be an even integer and let $n > 2$ be an odd integers. Find a formula for the number of elements of order 2 in $D_m \oplus D_n$.

Here, D_m has $m + 1$ elements of order 2, because $R_{180} \in D_m$. Then, D_n has n elements of order 2, because $R_{180} \notin D_n$. If an element $(a, b) \in D_m \oplus D_n$ has order two, then we must have one or both of a and b of order two, and any of a and b not of order two, being that of one, and there is only one element of order one; namely, the identity of either D_m or D_n, whichever applicable. So there are $m + n + mn$ elements of order two in $D_m \oplus D_n$, I think.

Problem 32

Let $(a_1, a_2, \ldots, a_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Give a necessary and sufficient condition for $|(a_1, a_2, \ldots, a_n)| = \infty$.

It may be reasonable to say that $\text{lcm}(|a_1|, \ldots, |a_n|) = \infty$ if and only if there exists an integer $i \in [1, n]$ such that $|a_i| = \infty$.

Problem 39

Suppose that $n_1, n_2, \ldots, n_k$ are positive even integers. How many elements of order 2 does $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ have? How many are there if we drop the requirement that $n_1, n_2, \ldots, n_k$ must be even?

If $n > 0$ is even, then Z_n has exactly one element of order 2; namely, n/2. So if $n_1, \ldots, n_k > 2$ are even, then there are

$$\binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k} = 2^k - \binom{k}{0} = 2^k - 1.$$

elements of order 2 in $Z_{n_1} \oplus \cdots \oplus Z_{n_k}$. Dropping the even requirement, if $0 \leq j \leq k$ is the number of integers in $\{n_i\}_{i=1}^k$ that are even, then there would be $2^j - 1$ elements of order 2, because there is no element of order 2 in Z_n when n is odd.

Problem 49

let p be a prime. Prove that $Z_p \oplus Z_p$ has exactly $p + 1$ subgroups of order p.

Letting $(i,j) \in Z_p \oplus Z_p$, we have $\langle (i,j) \rangle$ as a cyclic subgroup of $Z_p \oplus Z_p$ of order p whenever i and j are not both zero. So to count the number of such subgroups, we need to avoid redundant cases. Let us start by counting $\langle (i,0) \rangle$ and $\langle (0,i) \rangle$ with $i \neq 0$. This gives us two subgroups of order p. We then get the rest of the subgroups by counting $\langle (i,j) \rangle$ for all cases such that neither i nor j is zero, and $|i-j| = 0, 1, \ldots, p-2$. In total, we have $p-1+1+1 = p+1$ subgroups of order p.

The back of the book gives a much more elegant answer.

Problem 56

Let p and q be odd primes and let m and n be positive integers. Explain why $U(p^m) \oplus U(q^n)$ is not cyclic.

By Carl Gauss and Problem 14, we have

$$U(p^m) \oplus U(q^n) \approx Z_{p^m - p^{m-1}} \oplus Z_{q^n - q^{n-1}}.$$

Now notice that $p^m - p^{m-1} \geq 2$. The same can be said of $q^n - q^{n-1}$. Now simply realize that $Z_i \oplus Z_j$ is not cyclic for all $i, j \geq 2$ by a proof similar to that given in problem 5.