Section 2.3 Exercises
Hertein's Topics In Algebra

Spencer T. Parkin

February 28, 2016

Problem 8

If G is a finite group, show that threre exists a postive integer N such that $a^N = e$ for all $a \in G$.

It is not hard to show that for every $a \in G$, there exists an integer $k(a)$ such that $a^{k(a)} = e$. Further, $a^{nk(a)} = e$ for every integer n. Now let

$$N = \prod_{a \in G} k(a).$$

Problem 11

If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

Clearly G has an odd number of non-identity elements. Pluck such an element from G. If $a^2 = e$, we're done. If not, pluck its inverse out of G as well. This leaves us yet a smaller pool of odd elements to choose from. Continue this process until we either find an element being its own inverse, or we're left with just one non-identity element. Clearly this last remaining non-identity element must be its own inverse.

Problem 14

Suppose a finite set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.

If G is a singleton set, then its sole element must be identity, and we're done. If not, then it is not as yet clear that G has an identity element. Letting a be any element of G, consider the subset $\{a^i\}_{i=1}^{\infty}$. Clearly, since G is finite, this is a finite subset of G; and therefore, there exists $0 < i < j$ such that $a^i = a^j$. It follows that

$$a^i = a^i a^{j-i},$$

and we claim that a^{j-i} is an identity element. To substantiate this claim, let b be any element of G, and write

$$ba^{j-i} = c.$$

Multiplying both sides by a^i on the right, we obtain

$$ba^j = ca^i,$$

and then by the right-cancellation property, $b = c$. Similarly, we can show that a^{j-i} is an identity element on the left using the left-cancellation proprety.

What remains to be shown is that every element has a multiplicative inverse. Knowing now that there is an identity, for any $a \in G$, and by the proof we used to show its existence, we have $a^n = e$ for some positive integer n. (We found $n = j - i$ in one case above.) We can then claim that $a^{n-1} = a^{-1}$.

Exercise 15

Show that the nonzero integers less than and relatively prime to n for a group under multilication mod n.

(I'm only doing part (b) as it is a generalization of part (a).)

Let's start with closure. Letting $S(n) = \{0 < x < n | (x, n) = 1\}$, it is clear that for all $x, y \in S(n)$, that $(xy, n) = 1$, but we may have $xy \geq n$. Noting that there exist integers $u, v \in \mathbb{Z}$ such that

$$xyu + nv = 1,$$

we also note that

$$1 = (xy + kn - kn)u + nv = (xy + kn) + (-ku + v)n,$$

showing that, for all integers k, we have $(xy + kn, n) = 1$. We now have closure.

If we can now show that the cancellation law holds, then the problem goes through by Problem 14. To that end, for appropriate $x, y, z \in S(n)$, write

$$xy \equiv xz \pmod{n}.$$

This means that $n | x(y - z)$. But since $(x, n) = 1$, we must have $n | (y - z)$, and therefore

$$y \equiv z \pmod{n}.$$

(Recall Lemma 1.3.3, part 4.)

Exercise 26

Part (a)

Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$. G forms a group relative to matrix multiplication. What is $o(G)$?

We find $|G|$ by counting matrices of the said dimension and then subtracting from that the number of such being singular. Clearly there are p^4 matrices of the desired dimension. How many of them are singular? The singularity of a 2×2 matrix occurs whenever a row (column) is a scalar multiple of the other row (column). Consider the following expression.

$$(1)p^2 + (p - 1)p + (p - 1)p + (p - 1)^2 p.$$

This expression, having 4 terms, represents 4 cases. In the first case, one row is zero, leaving p^2 choices for the other row. In the second case, a row is axis-aligned in $p - 1$ ways with p ways the other row is zero or parallel to it. The third cases is counted like the second, but using the other axis. In the fourth case, there are $(p - 1)^2$ ways a row is non-zero and non-axis-aligned with p ways the other row is zero or parallel to it.

Putting it all together, we get

$$|G| = p^4 - p^3 - p^2 + p.$$

Part (b)

Let H be the subgroup of the G of part (a) defined by

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \,\middle|\, ad - bc = 1 \right\}.$$

What is $o(H)$?

Figure it out...