Algebra: Chapter 0 Exercises

Chapter 2, Section 1

David Melendez

May 21, 2017

Problem 2.2. If $d \leq n$, then S_n contains elements of order d.

Proposition. Let c_d, called a *d-cycle* in S_n, be defined as follows:

$$c_d(m) = \begin{cases} d & m = 1 \\ d-1 & 1 < m \leq d \\ m & m > d \end{cases}$$

For example, if we're working in S_6, then $c_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix}$.
Then $|c_d| = d$ for $1 \leq d \leq n$.

Proof. Note that if $0 < k < d$, then $c_d^k(d) = d - k \geq 1$ (c_d^k never "reaches" the point at which it cycles from 1 to d since $k < d$), so $|c_d| \geq d$. Then, we have, for $m \leq d$,

$$\begin{aligned} c_d^d(m) &= (c_d^m \cdot c_d^{d-m})(m) \\ &= c_d^{d-m}(d) \\ &= d - (d - m) \\ &= m \end{aligned}$$

Clearly $c_d^d(m) = m$ if $m > d$, so c_d^d is the identity, as desired. □

Problem 2.5. Describe generators and relations for all dihedral groups D_{2n}.

Solution. We will define the dihedral group D_{2n} as follows:

$$D_{2n} = \left\langle x, y \mid x^2 = y^n = (xy)^2 = e \right\rangle$$

Proposition. With this definition of D_{2n}, every combination $x^{i_1}y^{i_2}x^{i_4}y^{i_5}\cdots$ equals x^iy^j for some $0 \leq i \leq 1, 0 \leq j < n$.

Proof. We will use induction on m, the number of elements we're composing.
The cases for $0 \leq m \leq 2$ are obvious.
Suppose this reduction holds for m. Then, if m is odd, we have

$$\begin{aligned}\left(x^{k_1}y^{k_2}\cdots x^{k_m}\right)y^{k_{m+1}} &= x^iy^jy^{k_{m+1}} \\ &= x^iy^{j+k_{m+1}}\end{aligned}$$

The case where m is even is more interesting. First, we will establish the following based off of the third relation:

$$\begin{aligned}(xy)^2 = e \implies xyxy &= e \\ \implies x(yxy) &= e \\ \implies x^{-1} &= yxy \\ \implies yx &= x^{-1}y^{-1} \\ &= xy^{n-1}\end{aligned}$$

Now, suppose m is even. We then have, with $\leq i \leq 1$, $0 \leq j < n$, and $0 \leq k \leq 1$:

$$\left(x^{k_1}y^{k_2}\cdots x^{k_{m-1}}y^{k_m}\right)x^{k_{m+1}} = x^iy^jx^k$$

Since every other case is trivial, we will assume $0 \neq j \neq n$ and $k = 1$. Additionally, we will assume wlog that $j < n$. Then, we have

$$\begin{aligned}x^iy^jx^k &= x^iy^jx \\ &= x^iy^{j-1}(yx) \\ &= x^iy^{j-1}xy^{n-1} \\ &= x^iy^{j-2}xy^{2n-2} \\ &= x^iy^{j-2}xy^{n-2} \\ &= x^iy^{j-3}xy^{n-3} \\ &= \cdots \\ &= x^iy^0xy^{n-j} \\ &= x^{i+1}y^{n-j}\end{aligned}$$

as desired. ∎

∎

Problem 2.10. Prove that $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

Proposition. $\mathbb{Z}/n\mathbb{Z}$ consists exactly of the elements $S = \{[0]_n, [1]_n, \ldots [n-1]_n\}$.

Proof. First, suppose $[a]_n, [b]_n \in S$ and (without loss of generality) $a < b$. Then, since $b - a < n$, we have $n \nmid b - a$, and so $[a]_n$ and $[b]_n$ (and hence all elements of S) are distinct. Now, suppose $c \geq n$. Then we have, for some positive integers $q \geq 1$ and $0 \leq r < n$, $c = qn + r$. Hence $c - r = qn$, so $c \equiv r \mod n$. In other words, $[c]_n = [r]_n$ with $r < n$, completing the proof that $\mathbb{Z}/n\mathbb{Z} = S$. $\square$

Problem 2.11. The square of every odd integer is congruent to 1 modulo 8.

Solution. Let $n \geq 0$ be an integer. We will prove that $(2n+1)^2 \equiv 1 \mod 8$.
Note that $4x \equiv 0 \mod 8$ if x is even, and that

$$\begin{aligned} (2n+1)^2 &= 4n^2 + 4n + 1 \\ &= 4n(n+1) + 1 \end{aligned}$$

If $n = 2m + 1$ is odd, then we have

$$\begin{aligned} n(n+1) &= (2m+1)(2m+2) \\ &= 2(2m+1)(m+1) \\ &\equiv 0 \mod 2 \end{aligned}$$

Similarly, if $n = 2m$ is even, then we have

$$\begin{aligned} n(n+1) &= 2m(2m+1) \\ &\equiv 0 \mod 2 \end{aligned}$$

Thus $n(n+1)$ is even, giving us $4n(n+1) \equiv 0 \mod 8$, and hence

$$\begin{aligned} (2n+1)^2 &= 4n(n+1) + 1 \\ &\equiv 1 \mod 8 \end{aligned}$$

$\blacksquare$

Problem 2.12. There are no nonzero integers a, b, c such that $a^2 + b^2 = 3c^2$.

Solution. I'll write this one down later. Essentially, you work in $\mathbb{Z}/4\mathbb{Z}$ (as given in the text as a hint) split the problem into cases, and deduce an even-odd contradiction between $a^2 + b^2$ and $3c^2$. $\blacksquare$

Problem 2.13. There exist integers a and b such that

$$am + bn = 1$$

iff $\gcd(m, n) = 1$.

Solution. First suppose $\gcd(m, n) = 1$. By Corollary 2.5, we know that $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$, and hence

$$am \equiv 1 \mod n$$

for some integer a. It then follows that

$$am = bn + 1$$

for some integer b, and so

$$am - bn = 1$$

as desired.
For the proof in the other direction, suppose there exist integers a and b such that

$$am + bn = 1$$

Then we have

$$am = 1 - bn$$

. Suppose, for the sake of contradiction, that $\gcd(m, n) = d > 1$. We then have

$$\frac{am}{d} = \frac{1}{d} - \frac{bn}{d}$$
$$\frac{am}{d} + \frac{bn}{d} = \frac{1}{d}$$

The LHS is an integer since $d|m$ and $d|m$, but the (nonzero) RHS is not since $d > 1$. Absurd! ■

Problem 2.14. Show that multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation.

Solution. First, we shall prove a useful intuition regarding modulus.

Proposition. If $a \equiv b \mod n$, then there exist integers $k_1, k_2 \geq 0$ and r with $0 \leq r < n$ such that

$$a = k_1 n + r$$
$$b = k_2 n + r$$

Proof. Recall that $\mathbb{Z}/n\mathbb{Z}$ consists entirely of the equivalence classes of the numbers in the set of nonnegative integers up to but not including n. Thus, if $a \equiv b \mod n$, there exists an r with $0 \leq r < n$ such that

$$n|a - r$$
$$n|b - r$$

Hence, we have, for some nonnegative integers k_1, k_2:

$$k_1 n = a - r$$
$$k_2 n = b - r$$

Therefore

$$\begin{aligned} a &= k_1 n + r \\ b &= k_2 n + r \end{aligned}$$

as desired. ∎

With this, we can show that multiplication on $\mathbb{Z}/n\mathbb{Z}$ is well-defined.

Proposition. If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then $ab \equiv a'b' \mod n$.

Proof. Suppose $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Then, by the lemma above, we have:

$$\begin{aligned} a &= k_1 n + r \\ a' &= k_2 n + r \\ b &= \ell_1 n + s \\ b' &= \ell_2 n + s \end{aligned}$$

Next, consider the product ab:

$$\begin{aligned} ab &= (k_1 n + r)(\ell_1 n + s) \\ &= k_1 \ell_1 n^2 + k_1 s n + \ell_1 r n + rs \\ &= (k_1 \ell_1 n + k_1 s + \ell_1 r) n + rs \\ &\equiv rs \mod n \end{aligned}$$

Similarly, for $a'b'$,

$$\begin{aligned} a'b' &= (k_2 n + r)(\ell_2 n + s) \\ &= k_2 \ell_2 n^2 + k_2 s n + \ell_2 r n + rs \\ &= (k_2 \ell_2 n + k_2 s + \ell_2 r) n + rs \\ &\equiv rs \mod n \end{aligned}$$

Hence $ab \equiv a'b' \mod n$ by transitivity. ∎

∎