Homework #7

Problems to hand in on Thursday, March 21, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) Every group G such that $x^2y^2 = (xy)^2$ for all $x, y \in G$ must be abelian.

Solution.

2) Let $x, y \in G$. Then

$$yx = (x^{-1}x)yx(yy^{-1}) = x^{-1}(xy)^2y^{-1} = x^{-1}x^2y^2y^{-1} = xy.$$

3) Every group of order n containing an element of order n is abelian.

Solution. If G is a group of order n containing an element g of order n, we will show that G is cyclic and generated by g, and thus abelian. To do that, just consider the cyclic subgroup generated by g. This is a subgroup with n distinct elements: indeed, given $1 \leqslant m \leqslant k \leqslant n$, if $g^m = g^k$, then $g^{k-m} = g^k\,(g^m)^{-1} = e$, where e is the identity. But n was the smallest positive integer such that $g^n = e$, so we must have $m = k$. Now since $\langle g \rangle$ has n elements, they must be all the elements if G, and $G = \langle g \rangle$ is abelian.

4) Let p be a prime integer, and consider the group $\mathrm{GL}_2(\mathbb{Z}_p)$ of invertible 2×2 matrices with entries in $\mathbb{Z}_p$.

   a) Prove that for any nonzero column $\begin{bmatrix} a \\ b \end{bmatrix}$, the matrices $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ that are noninvertible are precisely those for which there exists n such that $\begin{bmatrix} c \\ d \end{bmatrix} = n \begin{bmatrix} a \\ b \end{bmatrix}$.

   b) Show that the set of upper triangular invertible matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ forms a subgroup of order $p(p-1)^2$, which is non-abelian when $p \neq 2$.

   c) Compute the order of $\mathrm{GL}_2(\mathbb{Z}_p)$.

   d) Show that the diagonal invertible matrices form an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order $(p-1)^2$.

   e) Find an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order p. Make sure to show this is a subgroup.

Solution.

(a) A matrix is a unit if and only if it is invertible, which happens if and only if its columns are linearly independent (217 to the rescue!). Since we are assuming the first column is nonzero, the matrix fails to be invertible if and only if the second column is a multiple of the first.

(b) The upper triangular matrices again must have nonzero entries on the diagonal (since the determinant is nonzero) but the upper right entry can be arbitrary. There are $(p-1)^2 p$ such matrices. The product of upper triangular matrices is upper triangular, the inverse of an upper triangular matrix is upper triangular, and the identity is upper triangular. For example,

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}^{-1} = (ac)^{-1} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix}.$$

To see this is not abelian, just note that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(c) For each nonzero first column, there are choices of a second column that make an invertible matrix – all columns except the p multiples of the first column. There are $p(p-1) = p^2 - 1$ choices for the first column, and $p(p-1) - (p-1) = p^2 - p$ for the second. There are $p^2(p-1)^2$ elements in $\mathrm{GL}_2(\mathbb{Z}_p)$.

(d) We need to have nonzero elements on the diagonal (or the determinant would be zero). There are $(p-1)^2$ of these. It's easy to check by direct computation that diagonal matrices commute with each other, the product of diagonal matrices is a diagonal matrix, and that the inverse of a diagonal matrix is diagonal. The identity matrix is a diagonal matrix.

(e) The upper triangular invertible matrices of the form

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix},$$

where $a \in \mathbb{Z}_p$ can be any element, form an abelian subgroup with p elements, since

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix}.$$

Note that this subgroup is then isomorphic to $\mathbb{Z}_p$.

5) A polygon is regular if all the sides have the same length and all the angles have the same measure. The regular n-gon has n sides. For example, a regular 4-gon is a square. For each $n \geqslant 3$, D_n denotes the group of symmetries of the regular n-gon. Fix a regular n-gon in the Cartesian plane so that its vertices are equidistant from the origin and one lies on the x-axis.

Theorem: $|D_n| = 2n$.

(a) The group D_n contains an element r of order n. Describe it.

(b) For each edge of the n-gon, the group D_n contains a particular element of order 2 that corresponds to some reflection. Similarly, for each vertex of the n-gon, the group D_n

contains a particular element of order 2 that corresponds to some reflection. Describe these elements. Explain why these give you a total of n distinct reflections. Hint: you want to distinguish between the cases when n is even or odd.

(c) Show that D_n can be generated by just one rotation and one reflection.

Solution.

(a) The clockwise rotation by $\frac{2\pi}{n}$ degrees.

(b) For each edge of the n-gon, the reflection along the line that is perpendicular to that side and that goes through the center of the n-gon gives an element of D_n. If n is even, each side has a corresponding parallel side, and these give the same reflection, so we just described a total of $n/2$ reflections; if n is odd, these are n distinct reflections.

Similarly, for each vertex of the n-gon, the refection along the line that goes through that vertex and the center of the n-gon gives an element of D_n. When n is even, each such line goes through two vertices, so we only described $n/2$ more reflections. When n is odd, there are again n distinct reflections we write this way, but they are the same n reflections we described before.

Either way, there are n reflections in D_n.

(c) Fix one of the reflections l from part b, and the rotation r from part (a).Then r generates a subgroup that contains all the rotations that are isometries of the n-gon, and the remaining reflections can be obtained by composing l with $r, r^2, \ldots, r^{n-1}$. Notice also that $lr^k = r^{n-k}l$. Now we just need to notice these are $n-1$ distinct elements, and together with the identity they make the whole group. So

$$D_n =< r, l > .$$