Math 30810 Honors Algebra 3
Homework 7

Andrei Jorza

Due in class on Wednesday, October 30

Do 5.

1-2 (Counts as 2 problems, and we'll use it in Galois theory next semester) Let $p > 2$ be a prime number and $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\}$, a group under matrix multiplication. Let $H < G$ be the subgroup of diagonal matrices.

(a) Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and define $N_a = \left\{ \begin{pmatrix} a^k & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/p\mathbb{Z}, k \in \mathbb{Z} \right\}$. Show that $N_a \lhd G$.

(b) If a normal subgroup N of G contains a matrix of the form $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ show that N also contains the matrix $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$. [Hint: Use that N is normal when $x \neq 1$ and that N is a subgroup when $x = 1$.]

(c) If N is a normal subgroup of G show that there exists $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ (necessarily of the form $a = g^k$ for a primitive root g mod p and an exponent k) such that $H \cap N$ is the set of matrices of the form $\begin{pmatrix} a^m & 0 \\ 0 & 1 \end{pmatrix}$, with $m \in \mathbb{Z}$. [Hint: You need to use that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.]

(d) Show that if a is as in part (c) then either $N = N_a$ or $N = \{I_2\}$. [Hint: Use that N is normal.]

Remark: We'll use this exercise in Galois theory next semester so I recommend you do it.

3. Let $G = \langle g \rangle$ be a cyclic group of order n. Recall that φ is Euler's function defined as $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ equals the number of integers $1 \leq k < m$ which are coprime to m.

(a) Show that g^k has order d if and only if $k = nr/d$ for r coprime to d.

(b) For a divisor $d \mid n$ show that there are exactly $\varphi(d)$ elements of G of order exactly d. (In particular G has exactly $\varphi(n)$ generators.)

(c) Deduce the identity $\displaystyle\sum_{d|n} \varphi(d) = n$. [Hint: Apply part (a) to all the divisors of n.]

Remark: There's a procedure by which the equations $\sum_{d|n} \varphi(d) = n$ for all positive integers n can be considered a system of equations with unknowns $\varphi(d)$ and one can actually solve for $\varphi(n)$ and obtain the formula we got in class. This is called Möbius inversion. We'll actually use Möbius inversion next semester in Galois theory to compute cyclotomic polynomials.

4. Consider the complex number $\zeta = e^{2\pi i/10}$ which generates the cyclic group $G = \langle \zeta \rangle$ of order 10. Show that the only homomorphisms $f : S_3 \to G$ are the trivial homomorphism and the sign homomorphism $\varepsilon(\sigma) \in \{-1, 1\}$. (Note that $\zeta^5 = -1$ so $\{-1, 1\} \subset \langle \zeta \rangle$.) [Hint: what is $f(A_3)$?]

5. Write $\mathbb{F}_2$ instead of $\mathbb{Z}/2\mathbb{Z}$.

   (a) Show that $\mathrm{GL}(2, \mathbb{F}_2)$ permutes the three nonzero vectors in $\mathbb{F}_2^2$.

   (b) Deduce that $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$.

6. Let $n \geq 3$ be an integer. The dihedral group D_n with $2n$ elements is

$$D_n = \{1, R, R^2, \ldots, R^{n-1}, F, FR, \ldots, FR^{n-1}\}$$

   satisfying $\mathrm{ord}(R) = n$, $\mathrm{ord}(F) = 2$ and $FRF = R^{n-1}$.

   (a) Show that D_n is a group isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ consisting of matrices of the form $\begin{pmatrix} \pm 1 & x \\ 0 & 1 \end{pmatrix}$ where $x \in \mathbb{Z}/n\mathbb{Z}$.

   (b) Suppose $a, b \in \mathbb{Z}/n\mathbb{Z}$. Show that R^a and FR^b generate D_{2n} (i.e., $D_{2n} = \langle R^a, FR^b \rangle$) if and only if $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. [Hint: Show that in an arbitrary product of R^a-s and FR^b-s and their inverses you can collect all the F-s on the left side.]

7. Recall from class that the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generate $\mathrm{SL}(2, \mathbb{Z})$.

   (a) Show that $\mathrm{SL}(2, \mathbb{Z}) = \langle S, ST \rangle$ and that the two generators S and ST have orders 4 respectively 6.

   (b) (Do either this or the next part) Show that the only homomorphism $f : \mathrm{SL}(2, \mathbb{Z}) \to \mathbb{Z}/7\mathbb{Z}$ is the trivial homomorphism. [Hint: It's enough to see where the generators go.]

   (c) (Do either this or the previous part) Show that every homomorphism $f : \mathrm{SL}(2, \mathbb{Z}) \to \mathbb{C}^\times$ has image $\mathrm{Im}\, f \subset \mu_{12} = \{z \in \mathbb{C}^\times \mid z^{12} = 1\}$.