Math 30810 Honors Algebra 3
Homework 7

Andrei Jorza

Due at noon on Thursday, October 13

Do any 8 of the following questions. Artin a.b.c means chapter a, section b, exercise c.

1-2 (Counts as 2 problems) 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 $p > 2$ be a prime number. Show by induction that if $n \geq 0$ and $p \nmid m$ then:

$$(1+p)^{p^n m} \equiv 1 + mp^{n+1} \pmod{p^{n+2}}$$

4. Let $p > 2$ be a prime number. Show that if g is a primitive root modulo p then $a = g^{p^{n-1}}(1+p)$ is a primitive root modulo p^n, i.e., $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ has order $\varphi(p^n)$ and therefore $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic generated by a. [Hint: Use the previous exercise.]

5. 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.

6. 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 $f(A_3)$?]

7. (a) Suppose $p \equiv 3 \pmod 4$ is a prime. If $y \equiv x^2 \pmod p$ show that $x \equiv \pm y^{(p+1)/4} \pmod p$. [Hint: start by showing that $x^2 \equiv y \pmod p$ can have at most 2 solutions.]

   (b) Consider $p = 503$ and $q = 991$, both $\equiv 3 \pmod 4$. I tell you that $x^2 \equiv 76472 \pmod{pq}$. What is $x \mod pq$? [Feel free to use wolfram alpha for computations. I'm giving you that $991 \cdot 67 - 132 \cdot 503 = 1$. It's easier to use the Chinese Remainder Theorem.]

   Remark: Rabin's cryptosystem sends x to $x^2 \mod pq$ for two primes $p \neq q$, both $\equiv 3 \pmod 4$, and you just produced a decryption algorithm.

8. (a) Show that if $f \in \mathrm{Aut}(S_3)$ then $f(\sigma) \in \{(12), (13), (23)\}$ and $f(\tau) \in \{(123), (132)\}$. [Recall that $\sigma = (12)$ and $\tau = (123)$ generate S_3.]

   (b) Deduce that $\mathrm{Aut}(S_3) \cong S_3$. [Hint: Use part (a) to show that $\mathrm{Aut}(S_3)$ has at most 6 elements. What is $\mathrm{Inn}(S_3) \subset \mathrm{Aut}(S_3)$?]

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

10. Let $H = \mathbb{Z}/2\mathbb{Z}$ and $N = \mathbb{Z}/8\mathbb{Z}$ and consider $\phi : H \to \mathrm{Aut}(N)$ defined as $\phi(x) = 3x$. Consider $R, F \in G := N \rtimes_\phi H$ defined as $R = (0, 1)$ and $F = (1, 0)$. Show that F and R generate G, F has order 2, R has order 8 and $FRF = R^3$.