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.

Proof. (a): Write $m(a, b) = \begin{pmatrix} a & b \\ & 1 \end{pmatrix}$. Look at the map $f : G \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $f(m(a, b)) = a$. By inspection this is a homomorphism. Moreover, N_a is defined as $N_a = f^{-1}(\langle a \rangle)$. Suppose $x \in N_a = f^{-1}(\langle a \rangle)$ and $g \in G$. Then $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(x) \in \langle a \rangle$ since the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is abelian. It follows that $gxg^{-1} \in f^{-1}(\langle a \rangle) = N_a$ and so N_a is normal.

Remark: In fact more generally the preimage of any normal group is also normal.

(b): If N contains the matrix $m(x, y)$ with $x \neq 1$ then, as N is normal in G, it also contains the matrix

$$m(1, u)m(x, y)m(1, -u) = m(x, y - (x - 1)u)$$

If $x \neq 1$ it follows that the map $u \mapsto y - (x - 1)u$ is bijective and so taking $u = y/(x - 1)$ yields that N contains the matrix $m(x, 0)$ as desired. If $x = 1$ then N also contains the power $m(1, y)^p = m(1, py) = I_2$.

(c): Suppose N is now normal in G. Then $f(N)$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. This group is cyclic and we know that every subgroup of a cyclic group is cyclic from a previous homework. Therefore $f(N) = \langle a \rangle$ for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. This means that for each exponent k the subgroup N contains an element of the form $m(a^k, b)$.

Part (b) applied to N then shows that N contains $m(a^k, 0)$ for each k. Necessarily $H \cap N_a$ is of the desired form.

(d): First, by definition of a, $N \subset N_a$. If $m(a^k, 0) \in N$ then $m(1, u)m(a^k, 0)m(1, -u) = m(a^k, (1 - a^k)u) \in N$. If $a^k \neq 1$ it follows as in part (b) that $N_a \subset N$. It follows that $N = N_a$.

Suppose that $a \neq 1$. We still need to show that all matrices of the form $m(1, b)$ are in N. But from the previous line we know that if a has order d then $m(a^{d-1}, x) \in N$ and so $m(1, x) = m(a^{d-1}, x)m(a, 0) \in N$. We deduce that $N = N_a$.

Finally, suppose $a = 1$. If $N \neq \{I_2\}$ then N contains a matrix of the form $m(1, b)$ for some $b \neq 0$. Then $m(1, b)^r = m(1, rb) \in N$ and varying r we deduce that $N_1 \subset N$. Again we conclude that $N = N_1$. □

3. Let $p > 2$ be a prime number. Show by induction that if $n \geq 0$ and $p \nmid m$ then:

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

Proof. We'll prove by induction on n. If $n = 0$ then $(1+p)^m = 1 + mp + \binom{m}{2}p^2 + \cdots \equiv 1 + pm \pmod{p^2}$. Suppose that $(1+p)^{p^n m} \equiv 1 + mp^{n+1} \pmod{p^{n+2}}$. Then $(1+p)^{p^n m} = 1 + mp^{n+1} + kp^{n+2}$. We now compute

$$\begin{aligned}(1+p)^{p^{n+1}m} &= (1 + mp^{n+1} + kp^{n+2})^p \\ &= (1 + p^{n+1}(m + kp))^p \\ &= 1 + p^{n+2}(m + kp) + \binom{p}{2}p^{2(n+1)}(m + kp)^2 + \cdots \\ &\equiv 1 + mp^{n+2} \pmod{p^{n+3}}\end{aligned}$$

which concludes the inductive step. □

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.]

Proof. Since $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = \varphi(p^n)$ it follows that the multiplicative order of a divides $\varphi(p^n)$. To check that it is equal to it we'll apply a problem from homework 6. We have to check that $a^{\varphi(p^n)/q} \not\equiv 1 \pmod{p^n}$ for every prime $q \mid \varphi(p^n) = p^{n-1}(p-1)$.

If $q = p$ we compute

$$a^{\varphi(p^n)/q} = a^{p^{n-2}(p-1)} = g^{p^{2n-3}(p-1)}(1+p)^{p^{n-2}(p-1)} \equiv (1+p)^{p^{n-2}(p-1)} \equiv 1 + (p-1)p^{n-1} \pmod{p^n} \not\equiv 1 \pmod{p^n}$$

since g has order $\mid \varphi(p^n)$ and also applying the previous problem.

If $q \mid p - 1$, then $\varphi(p^n)/q = p^{n-1}k$ where $k = (p-1)/q$. From the previous problem $(1+p)^{\varphi(p^n)/q} = (1+p)^{p^{n-1}k} \equiv 1 \pmod{p^n}$ and so

$$a^{\varphi(p^n)/q} \equiv g^{p^{n-1}k} \pmod{p^n}$$

If this were $\equiv 1 \pmod{p^n}$ it would also be $\equiv 1 \pmod{p}$ BUT

$$g^{p^{n-1}k} \equiv g^k \pmod{p}$$

(since $g^{p-1} \equiv 1 \pmod{p}$) which contradicts the fact that g has order $p - 1$ modulo p and therefore $g^k \not\equiv 1 \pmod{p}$ for $k = (p-1)/q$. □

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 $1 \le k < m$ 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.]

Proof. (a): The order of g^k from class is $n/(k,n)$ which is equal to d if and only if $(k,n) = n/d$. This means that $n/d \mid k$ and so $k = nr/d$ for some r. Moreover, $(k,n) = n(r,d)/d$ and so r must be coprime to d.

(b): Since $G = \{1, g, g^2, \ldots, g^{n-1}\}$ it follows that the elements of order d are those g^k with $0 \le k \le n-1$ such that $k = nr/d$ with r coprime to d. Equivalently the elements of order d are those $g^{nr/d}$ with $0 \le r < d$ with r coprime to d and by definition there's exactly $\varphi(d)$ such r.

(c): From a homework and from class any element of G has order $\mid n$. There's a total of n elements of G and each has order some divisor $d \mid n$. For each $d \mid n$ let G_d be the subset of G of elements of order d. Then G is a disjoint union of all G_d as $d \mid n$ (e.g., because in class we showed that having the same order is an equivalence relation and G_d are equivalence classes). We conclude that $n = |G| = \sum_{d|n} |G_d| = \sum_{d|n} \varphi(d)$. □

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 $f(A_3)$?]

Proof. Since $|f(A_3)| \mid |A_3| = 3$ from the first isomorphism therem but also $|f(A_3)| \mid 10$ as $f(A_3)$ is a subgroup of $\langle \zeta \rangle$, it follows that $f(A_3) = 1$. Recall that if $\sigma = (12)$ and $\tau = (123)$ then $A_3 = \{1, \tau, \tau^2\}$ and $S_3 = \{1, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\} = \{\sigma^a \tau^b \mid a = 0, 1, b = 0, 1, 2\}$. Since $f(\sigma^a \tau^b) = f(\sigma)^a$ it follows that f is uniquely determined by $f(\sigma)$. As $\sigma^2 = 1$ it follows that $f(\sigma)^2 = 1$ and $\langle \zeta \rangle$, being cyclic, contains exactly 2 elements whose square is 1 (e.g., from the previous problem is has $\varphi(2) = 1$ elements of order 2, plus the identity). Thus $f(\sigma) = \pm 1$.

If $f(\sigma) = 1$ then f is the trivial homomorphism. If $f(\sigma) = -1$ then $f(\sigma\tau^b) = -1$ and visibly $f = \varepsilon$. □

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.]

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

Proof. (a): If $u^2 \equiv v^2 \pmod p$ it follows that $p \mid u^2 - v^2 = (u-v)(u+v)$ and so $u \equiv \pm v \pmod p$. Thus to show that $x \equiv \pm y^{(p+1)/4} \pmod p$ it suffices to check that $x^2 \equiv y^{(p+1)/2} \pmod p$. But

$$y^{(p+1)/2} \equiv (x^2)^{(p+1)/2} \equiv x^{p+1} \equiv x^2 \pmod p$$

from Fermat's little theorem.

(b): From part (a) we know that $x \equiv \pm 76472^{(p+1)/4} \pmod p \equiv \pm 4$ and $x \equiv \pm 76473^{(q+1)/4} \pmod q \equiv \pm -34$. From homework 6 (explicit CRT) and the Bezout provided in the problem we know then that

$$x \equiv \pm 4 \cdot 991 \cdot 67 + \pm 34 \cdot 132 \cdot 503 \equiv \pm 2016, \pm 30687 \pmod{pq}$$

□

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 $\mathrm{Inn}(S_3) \subset \mathrm{Aut}(S_3)$?]

   Proof. (a): If f is an automorphism then $f(g^k) = f(g^k)$ so $g^k = 1$ iff $f(g)^k = 1$ so $f(g)$ and g have the same order. Now σ has order 2 so $f(\sigma)$ has order 2 so $f(\sigma)$ is one of the 3 transpositions in the list. Also τ has order 3 so $f(\tau)$ is one of the 2 3-cycles.

   (b): Since $f(\sigma)$ and $f(\tau)$ uniquely determine f as S_3 is generated by σ and τ, it follows that the total number of automorphisms is at most $3 \cdot 2 = 6$, with 3 choices for $f(\sigma)$ and 2 choices for $f(\tau)$. It's not guaranteed that all these 6 possibilities are realizable. However, $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) = S_3$ (from class) has 6 elements and $\mathrm{Inn}(S_3) \subset \mathrm{Aut}(S_3)$ where the RHS has at most 6 elements. Thus $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$. □

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

   Proof. (a): If $g \in \mathrm{GL}(2, \mathbb{F}_2)$ then g is invertible and so $gv = 0$ iff $v = 0$. If $X = \{(1, 0), (0, 1), (1, 1)\}$ are the 3 nonzero vectors in $\mathbb{F}_2^2$, it follows that $gx \in X$ for every $x \in X$. If $gx = gy$ for $x, y \in X$, again as g is invertible (in fact $\det(g) \in \mathbb{F}_2^\times = 1$ so $g^{-1} = g^*$ is the cofactor matrix directly) we deduce that $x = y$. Thus multiplication by g is injective on X so therefore it is also surjective, yielding a permutation of X.

   We know from class that multiplying matrices is the same as composing the linear maps they define so we deduce that $\mathrm{GL}(2, \mathbb{F}_2) \to \mathrm{Permutations}(X) = S_3$ is a homomorphism. The matrix $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ clearly yields a transposition in S_3 (interchanges $(0, 1)$ and $(1, 1)$ while the matrix $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ yields a different transposition. This means that the image of $\mathrm{GL}(2, \mathbb{F}_2)$ in S_3 is a group (as the image of a homomorphism) which contains 2 transpositions. From class we know the subgroups of S_3 and thus the image has to be all of S_3. Finally, what is the kernel of $\mathrm{GL}(2, \mathbb{F}_2) \to S_3$? If $gx = x$ for every $x \in X$ for some $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_2)$, then plugging this matrix into the 3 formulae we get that $a = d = 1$ and $b = c = 0$ so $g = I_2$. We 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 $FRF = R^3$.

    Proof. The multiplication map in G is $(0, x)(b, y) = (b, x + y)$ and $(1, x)(b, y) = (1 + b, x + 3y)$ which can be summarized as $(a, x)(b, y) = (a + b, x + 3^a y)$.

    Therefore $R^2 = (0, 1)(0, 1) = (0, 2)$ and by induction $R^k = (0, k)$ so R has order 8 as $k \in \mathbb{Z}/8\mathbb{Z}$. Also $F^2 = (1, 0)(1, 0) = (0, 0) = 1$. Finally, $FRF = (1, 0)(0, 1)(1, 0) = (1, 3)(1, 0) = (0, 3) = R^3$. Finally, $R \in N$ generates N as it has order 8 and similarly F generates H. Therefore F and R generate $NH = G$. □