Math 30810 Honors Algebra 3
Homework 5

Andrei Jorza

Due Thursday, September 29

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

1. Let G be a group and $g \in G$. Suppose $g^m = e$ and $g^n = e$ where m and n are coprime integers. Show that $g = e$.

   Proof. Bezout implies there exist p and q integers such that $pm+qn = 1$. Then $g = (g^m)^p(g^n)^q = 1$. □

2. Let G be a group.

   (a) Assume that H and K are subgroups and $|H| = |K| = p$ is a prime number. Show that either $H = K$ or $H \cap K = \{e\}$.

   (b) Let G be a group and $H_1, \dots, H_k$ be distinct subgroups of G. Suppose that each group H_i has order p, a fixed prime number. Show that $H_1 \cup \dots \cup H_k$ has exactly $(p-1)k+1$ elements.

   Proof. (a): From class $H \cap K$ is always a group, and will be a subgroup of H and K. The order of a subgroup divides the order of the group containing it so $|H \cap K| \mid |H|, |K|$ so either $|H \cap K| = 1$ in which case $H \cap K = \{e\}$ or $|H \cap K| = p$ in which case $H \cap K \subset H, K$ all have the same cardinality to $H = K = H \cap K$.

   (b): From part (a) we know that if $H_i \neq H_j$ then $H_i \cap H_j = \{e\}$. In the union $H_1 \cup \dots \cup H_k$, the only element that appears in more than one subgroup is e, which appears in all of them. Thus the total number of elements is $1 + (p-1)k$, each $H_i - \{e\}$ contributing $p-1$ elements to the union, and e being the $+1$. □

3. Suppose G is a finite group and p is a prime number such that every element $g \in G - \{e\}$ has order p. Show that $p - 1 \mid |G| - 1$. [Hint: use exercise 2.]

   Proof. There's a number of ways to write this. Here's the easiest: for $g \in G - \{e\}$ let $H_g = \langle g \rangle = \{e, g, g^2, \dots, g^{p-1}\}$ as $\mathrm{ord}(g) = p$. Pick $g_1 \in G - \{e\}$, then a $g_2 \in G - H_{g_1}$, then $g_3 \in G - (H_{g_1} \cup H_{g_2})$ and so on until there are no more elements to choose, i.e., $G = H_{g_1} \cup H_{g_2} \cup \dots \cup H_{g_k}$. By construction, $H_{g_i} \neq H_{g_j}$ when $g_i \neq g_j$ and each H_{g_i} is cyclic of order p. Exercise 2 then shows that $|G| = |H_{g_1} \cup \dots \cup H_{g_k}| = (p-1)k + 1$ and so $p - 1 \mid |G| - 1$. □

4. Let G be a group and suppose G contains an element of order n. Show that for every divisor $d \mid n$ the group G contains an element of order d. Deduce that if G has order p^n for some prime p, G contains an element of order p.

   Proof. From class we know that if g has order n then $g^{n/d}$ has order $n/(n, n/d) = n/(n/d) = d$.

   If G has order p^n pick any nontrivial element $g \in G - \{e\}$. Then $\mathrm{ord}(g) \mid |G| = p^n$ so $\mathrm{ord}(g) = p^k$ for some $k \geq 1$. Since $p \mid p^k$, the first part shows that G contains an element of order p. □

5. Let $p > q$ be prime numbers such that $q-1 \nmid p-1$, and suppose G is a group of order exactly pq. (E.g., G could have order 35.) Show that G contains an element of order p and an element of order q. [Hint: you may find exercises 3 and 4 useful.]

   Proof. Since $p > q$, $p-1 \nmid q-1$ as well. If $g \in G - \{e\}$, $\operatorname{ord}(g) \mid pq$ so $\operatorname{ord}(g) \in \{p, q, pq\}$ (since $g \neq e$, $\operatorname{ord}(g) \neq 1$). If $\operatorname{ord}(g) = pq$ then Exercise 4 implies the desired statement. We now argue by contradiction. Suppose G doesn't contain an element of order q ((the case of G not containing an element of order p being identical to this one). Then every $g \in G - \{e\}$ has order p (not 1, not q and not pq). Exercise 3 then implies that $p - 1 \mid |G| - 1 = pq - 1$. But then $p - 1 \mid (p-1)q + q - 1$ and so $p - 1 \mid q - 1$ which is impossible. □

6. (I encourage you to do this problem) Let $G = \mathrm{GL}_2(\mathbb{R})$ and H the subgroup of upper triangular matrices. Show that a complete set of representatives of G/H is given by the matrices

$$\left\{\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix} \mid x \in \mathbb{R}\right\} \sqcup \left\{\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\}$$

   (The proper interpretation of this is that the first set of matrices represents the real line and the antidiagonal matrix represents the "point at infinity", the quotient G/H being the projective line. This is important in representation theory.)

   Proof. First, we check that every matrix is in one of these cosets.

   If $g = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ is upper triangular then it is in the coset I_2 so let's assume now that $c \neq 0$. The coset gH contains $g\begin{pmatrix}x & y\\ & z\end{pmatrix} = \begin{pmatrix}ax & ay+bz\\ cx & cy+dz\end{pmatrix}$. If $a \neq 0$ we can take $x = 1/a$ and we can solve for y and z such that $ay + bz = 0$ and $cy + dz = 1$. Thus the coset gH contains the representative $\begin{pmatrix}1 & 0\\ c/a & 1\end{pmatrix}$ as desired. If $a = 0$, since $c \neq 0$ we can solve the system $bz = 1$, $cx = 1$ and $cy + dz = 0$ to get that gH contains the representative $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

   Finally, we need to show that no two representatives in the list lie in the same coset. But $gH = hH$ iff $gh^{-1} \in H$ and we notice that

$$\begin{pmatrix}1 & \\ x & 1\end{pmatrix}\begin{pmatrix}1 & \\ y & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & \\ x-y & 1\end{pmatrix} \notin H$$

   and

$$\begin{pmatrix}1 & \\ x & 1\end{pmatrix}\begin{pmatrix} & 1\\ 1 & \end{pmatrix}^{-1} = \begin{pmatrix} & 1\\ 1 & x\end{pmatrix} \notin H$$

   □

7. Artin 2.8.8 on page 73.

   Proof. From a previous exercise G contains an element g of order 5 as $|G| = 5^2$. Then $\langle g\rangle$ is a subgroup of order 5. If G is not cyclic then there is no element of order 25. Pick $h \in G - \langle g\rangle$. Since $\operatorname{ord}(h) \mid 25$ and the order is not 25 or 1, it follows that $\operatorname{ord}(h) = 5$. But then $\langle h\rangle$ is another subgroup of order 5, contradicting the assumption. □

8. Artin 2.8.10 on page 73.

Proof. For the counterexample look at $\langle(12)\rangle$ in S_3, of index 3 but not normal from the previous homework.

Supose $[G : H] = 2$. Then $G = H \sqcup cH$ is the disjoint union of the two cosets. Pick $g \in G$. We need to show that $gHg^{-1} \subset H$. Either $g \in H$ or $g \in cH$. If $g \in H$ then immediately $gHg^{-1} \subset H$ as H is a group. Otherwise $g = ch$ for some $g \in H$ and so $gHg^{-1} = chHh^{-1}c^{-1} \subset cHc^{-1}$. If $x \in H$ look at $cxc^{-1} \in G = H \sqcup cH$. As $c \notin H$ it follows that $cxc^{-1} \notin cH$ and so $cxc^{-1} \in H$ as desired. □

9. Artin 2.9.3 on page 73.

Proof. If $a = \overline{a_d a_{d-1} \dots a_1 a_0}_{(10)}$ then $a = \sum a_i 10^i = \sum a_i + \sum a_i(10^i - 1) = \sum a_i + \sum a_i 99\dots9$. □

10. Artin 2.8.6 on page 73.

Proof. We know that $\ker f$ is a subgroup of G so $a = |\ker f|$ divides 18 and $b = \operatorname{Im} f$ is a subgroup of G' so $|\operatorname{Im} f|$ divides 15. At the same time the first isomorphism theorem implies that $|G/\ker f| = |\operatorname{Im} f|$ and so $|\ker f||\operatorname{Im} f| = |G| = 18$. So we have $ab = 18$ with $b \mid 15$. Thus $b \mid (15, 18) = 3$. By assumption $b \neq 1$ as f is not trivial and so $b = 3$. Then $a = 6$.

□

11. (This was one is fun and jocular) Artin 2.M.16 on page 77. Artin says he learned of this from a paper of Mestre, Schoof, Washington and Zagier. The paper starts with the "motto": *Ah! La recherche. Du temps perdu.*

Proof. Yeah, I'm not writing this up. The group is trivial. □