Algebra I - Homework 4

Pablo Sánchez Ocal

October 14th, 2016

Exercise 1

Let G be a group with $H \leq G$ a subgroup with $[G : H] = n$ finite. We want to find a subgroup $N \leq H$ with $N \lhd G$ with $[G : N]$ finite.

Since $[G : H]$ is finite, consider G/H the set of cosets, of cardinal n. The action by translation:

$$\begin{array}{rcl} t \ : \ G \times G/H & \longrightarrow & G/H \\ (g, fH) & \longmapsto & (gf)H \end{array}$$

induces a homomorphism towards the group of permutations $S_{G/H} \cong S_n$, say $T : G \longrightarrow S_n$, since we can label the n different elements in $G/H = \{f_1H, \ldots, f_nH\}$, and then the element $g \in G$ can be identified with σ_g the permutation $\sigma_g(fH) = (gf)H$ (this identification yields indeed a permutation since it has $\sigma_{g^{-1}}$ inverse $\sigma_{g^{-1}}(fH) = (g^{-1}fH)$ with $g^{-1} \in G$). Moreover for any $g_1, g_2, f \in G$:

$$\begin{aligned} T(g_1g_2)(fH) &= \sigma_{g_1g_2}(fH) = (g_1g_2f)H = (g_1f)H(g_2f)H = \sigma_{g_1}(fH)\sigma_{g_2}(fH) = \\ &= T(g_1)(fH)T(g_2)(fH) \Longrightarrow T(g_1g_2) = T(g_2)T(g_2). \end{aligned}$$

hence T is indeed a homomorphism. Say $N = \ker(T) \leq G$, by the First Isomorphism Theorem, we have that $G/N \cong S$ for certain $S \leq S_n$. We claim that this N is what we need to solve the problem.

First, let $n \in N$, we have $T(n) = id_{G/H}$ hence:

$$H = T(n)(H) = nH \Longrightarrow n \in H \Longrightarrow N \leq H.$$

We also know that N is normal, $N \lhd G$, since it is the kernel of a homomorphism. Finally:

$$[G : N] = |G/N| = |S| \leq |S_n| = n!$$

which is finite, as desired.

Exercise 2

Show that every finite group G is isomorphic to a subgroup of A_k for some $k \in \mathbb{N}$.

For this, we will use Cayley's Theorem, which in particular states that every finite subgroup G is isomorphic to a subgroup of S_n with $|G| = n$. We call the monomorphism that induces such isomorphism $\iota : G \longrightarrow S_n$. Moreover, we have that $S_n \subset S_{n+2}$ in a natural way. We will define an monomorphism $\varphi : S_n \longrightarrow A_{n+2}$, and thus we will have a monomorphism $\varphi \circ \iota : G \longrightarrow A_{n+2}$, meaning that G is isomorphic to a subgroup of A_{n+2}, as desired (by the First Isomorphism Theorem if we are to precise everything).

The monomorphism φ is defined as:

$$\begin{array}{cccc} \varphi & : & S_n & \longrightarrow & A_{n+2} \\ & & \sigma & \longmapsto & \begin{cases} \sigma \text{ if } \sigma \text{ even} \\ \sigma(n+1, n+2) \text{ if } \sigma \text{ odd} \end{cases} \end{array}$$

where the injectivity is clear for even permutations and given by multiplication by $(n+1, n+2)$ for odd permutations (since $(n+1, n+2)$ commutes with every element of S_n and $(n+1, n+2)^2 = id_{S_{n+2}}$). To check that this is indeed a homomorphism, notice that for $\sigma, \tau \in S_n$ they either have the same parity or different parity:

$$\begin{cases} \varphi(\sigma)\varphi(\tau) = \sigma\tau = \varphi(\sigma\tau) \text{ if they have the same parity} \\ \varphi(\sigma)\varphi(\tau) = \sigma\tau(n+1, n+2) = \varphi(\sigma\tau) \text{ if they have different parity} \end{cases}$$

thus $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ in every case.

Exercise 3

To prove Burnside's Lemma, let G be a finite group acting on a finite set X. For notation, let $X^g = \{x \in X : gx = x\}$ for every $g \in G$ with $|X^g| = m_g$ by definition, let $G_x = \{g \in G : gx = x\}$ for every $x \in X$, let $\mathcal{O}_x = \{y \in X : \exists g \in G, y = gx\}$ for every $x \in X$.

Notice that:

$$x \in X^g \iff gx = x \iff g \in G_x$$

hence when we sum $\sum_{g\in G} m_g$, a point $x \in X$ is counted as many times as there are elements $g \in G$ that fix it, which is exactly $|G_x|$. Thus $\sum_{g\in G} m_g = \sum_{x\in X} |G_x|$. Using an alternative mathematical notation, we have proven that:

$$\sum_{g\in G} m_g = \sum_{g\in G} |X^g| = |\{(g, x) \in G \times X : gx = x\}| = \sum_{x\in X} |G_x|.$$

Once we have this, we can compute (since $|\mathcal{O}_x| = [G : G_x] = |G|/|G_x|$ by G finite):

$$\sum_{g\in G} m_g = \sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|} \implies \frac{1}{|G|}\sum_{g\in G} m_g = \sum_{x\in X} \frac{1}{|\mathcal{O}_x|}.$$

Now, suppose the action of G on X divides the latter into k disjoint orbits (an assumption we can do since both are finite), say $|\mathcal{O}_{x_1}|, \dots, |\mathcal{O}_{x_k}|$ for $x_1, \dots, x_k \in X$. We have $|X| = |\mathcal{O}_{x_1}| + \cdots + |\mathcal{O}_{x_k}|$, notice that since an element $x \in X$ can only belong to one orbit, that is $x \in |\mathcal{O}_{x_i}| = |\mathcal{O}_x|$ for some $1 \le i \le k$, and in particular $\sum_{x\in\mathcal{O}_{x_i}} 1 = |\mathcal{O}_{x_i}|$. Now:

$$\sum_{x\in X} \frac{1}{|\mathcal{O}_x|} = \sum_{x\in\mathcal{O}_{x_1}\cup\cdots\cup\mathcal{O}_{x_k}} \frac{1}{|\mathcal{O}_x|} = \sum_{i=1}^{k} \sum_{x\in\mathcal{O}_{x_i}} \frac{1}{|\mathcal{O}_{x_i}|} = \sum_{i=1}^{k} 1 = k$$

which is precisely the number of orbits.

Thus:

$$\frac{1}{|G|}\sum_{g\in G} m_g = \sum_{x\in X} \frac{1}{|\mathcal{O}_x|} = k, \text{ the number of orbits.}$$

Exercise 4

We want to find the number of possible different ways to paint the sides of a regular hexagon in three colors, saying that two coloring are the same if one can be obtained from the other by application of an element of D_6.

To use Burnside's Lemma, we first notice that without any restrictions, we have 6 sides in the hexagon and 3 colours, hence 3^6 possible coloring. Let X have as points all these different coloring, in particular $|X| = 3^6$. Second, notice that we identify two coloring as the same when they belong to the same orbit by the action of $G = D_6$ on X, where this action is the natural induced by D_6 onto the hexagon that determines an action on the sides of the hexagon, which are colored, meaning indeed an action on X. Suppose we have k such orbits, that is the number we want to find.

Thus for each of the 12 elements of D_6, we have to compute the number of points that it fixes. If we consider an hexagon flat on the base, starting on the right vertex, we can name the sides of the hexagon from 1 to 6 counterclockwise. Now, using the notation from Exercise 1.4 and Exercise 4.3, we have six rotations r_α with $\alpha \in \{0, \pi/3, 2\pi/3, \pi, 4\pi/3, 5\pi/3\}$, three mirror symmetries along the edges e_β with $\beta \in \{\pi/6, \pi/2, 5\pi/6\}$ and three mirror symmetries along the diagonals d_γ with $\gamma \in \{0, \pi/3, 2\pi/3\}$. In Table 1 we present the number of points fixed, where the computation of m_g for $g \in D_6$ is justified since for each set of related sides we have three choices for a color.

Element $g \in D_6$	Related sides	m_g
r_0	All independent	3^6
$r_{\pi/3}$	All related	3
$r_{2\pi/3}$	$1-3-5$, $2-4-6$	3^2
r_π	$1-4$, $2-5$, $3-6$	3^3
$r_{4\pi/3}$	$1-3-5$, $2-4-6$	3^2
$r_{5\pi/3}$	All related	3
$e_{\pi/6}$	1, $2-6$, $3-5$, 4	3^4
$e_{\pi/3}$	$1-3$, 2, $4-6$, 5	3^4
$e_{5\pi/6}$	$1-5$, $2-4$, 3, 6	3^4
d_0	$1-6$, $2-5$, $3-4$	3^3
$d_{\pi/3}$	$1-2$, $3-6$, $4-5$	3^3
$d_{2\pi/3}$	$1-4$, $2-3$, $5-6$	3^3

Table 1: Points fixed by the elements in D_6.

Thus applying:

$$k = \frac{1}{|G|} \sum_{g \in G} m_g = \frac{1}{24}(3^6 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 3 \cdot 3^4 + 3 \cdot 3^3) = 92,$$

the number of different coloring that we have.

Exercise 5

We want to find a Sylow subgroup of S_{2p} with p prime, $p > 2$.

We first notice that:

$$|S_{2p}| = (2p)! = (2p)(2p-1)\cdots\underbrace{(2p-(p-1))}_{p+1}\underbrace{(2p-p)}_{p}\cdots\underbrace{(2p-(2p-2))}_{2}\underbrace{(2p-(2p-1))}_{1}$$

and hence highest prime squared that divides $(2p)!$ is p^2 (because $p > 2$), in particular $p^2|(2p)!$ but $p^3 \nmid (2p)!$. Consider now $a = (2p, \ldots, p)$, $b = (p, \ldots, 1)$ elements of S_{2p}. They are disjoint and have order p, thus $ab = ba$ and:

$$S = \langle a, b\rangle = \{a^n b^m : n, m \in \mathbb{Z}\} = \langle a\rangle \times \langle b\rangle$$

is $S \leq S_{2p}$ with $|S| = |a||b| = p^2$. By the above, S is a Sylow p-subgroup.

Notice that it is important that $p > 2$: we have $4! = 4 \cdot 3 \cdot 2$ and thus it has $8 = 2^3 > 4 = 2^2$ as a divisor. Explicitly, in S_4 we have:

$$\langle (4,3), (2,1)\rangle \lneq D_4 \lneq S_4$$

with $|\langle (4,3), (2,1)\rangle| = 4$ and $|D_4| = 8$, in particular $\langle (4,3), (2,1)\rangle$ is not maximal, hence not a Sylow 2-subgroup.

Exercise 6

We want to show that groups G of order 28, 56 and 200 cannot be simple. The strategy that we will use is all three cases is the following: we will find a prime factor p dividing $|G|$ such that the Sylow p-subgroup, that exists by the First Sylow Theorem, is unique. To show uniqueness, we will use the Third Sylow Theorem, that gives us the possible numbers of such Sylow p-subgroups. Now by [1, Corollary 5.8 (iii), p. 95], if P is the only Sylow p-subgroup, then P is normal in G (because $P \cong gPg^{-1}$ for every $g \in G$, hence since $|gPg^{-1}| = |P|$ we have that gPg^{-1} is a Sylow p-subgroup, thus by uniqueness $P = gPg^{-1}$). Hence, G cannot be simple.

1. $|G| = 28$: we have $28 = 2 \cdot 2 \cdot 7$, in particular by the First Sylow Theorem we know that there exists a Sylow 7-subgroup of G and by the Third Sylow Theorem we know that the number of Sylow 7-subgroups of G divides 28 and is of the form $7 \cdot k + 1$ for $k \in \mathbb{N}$. Now:

$$1|28, \quad 8 \nmid 28, \quad 15 \nmid 28, \quad 22 \nmid 28,$$

   and obviously for $k > 3$ we have $(7 \cdot k + 1) \nmid 28$. Thus we have a unique Sylow 7-subgroup, which must be normal.

2. $|G| = 56$: we have $56 = 2 \cdot 2 \cdot 2 \cdot 7$. By the First Sylow Theorem we know that there exists a Sylow 7-subgroup of G and by the Third Sylow Theorem we know that the number of Sylow 7-subgroups of G divides 56 and is of the form $7 \cdot k + 1$ for $k \in \mathbb{N}$. Now:

$$1|56, \quad 8|56, \quad 15 \nmid 56, \quad 22 \nmid 56, \quad 29 \nmid 56$$

   and obviously for $k > 4$ we have $(7 \cdot k + 1) \nmid 56$. Thus we either have 1 or 8 Sylow 7-subgroups.

   Analogously, by the First Sylow Theorem we know that there exists a Sylow 2-subgroup of G and by the Third Sylow Theorem we know that the number of Sylow 2-subgroups of G divides 56 and is of the form $2 \cdot k + 1$ for $k \in \mathbb{N}$. Now:

$$1|56, \quad 3 \nmid 56, \quad 5 \nmid 56, \quad 7 \nmid 56, \quad 9|56, \quad 11 \nmid 56, \quad 13 \nmid 56, \quad 15 \nmid 56,$$
$$17 \nmid 56, \quad 19 \nmid 56, \quad 21 \nmid 56, \quad 23 \nmid 56, \quad 25 \nmid 56, \quad 27 \nmid 56, \quad 29 \nmid 56$$

   and obviously for $k > 14$ we have $(2 \cdot k + 1) \nmid 56$. Thus we either have 1 or 9 Sylow 2-subgroups.

   If we have more than 1 Sylow p-subgroup for both $p = 2, 7$, since the size of the Sylow 2-subgroups is 8 and the size of the Sylow 7-subgroups is 7, we must have at least

$$8 \cdot (7 - 1) + 9 \cdot (8 - 1) = 111 \text{ different elements in } G.$$

   This is a contradiction with $|G| = 56$. We hence have 1 Sylow p-subgroup for either $p = 2$ or $p = 7$ (maybe both), which must be normal.

3. $|G| = 200$: we have $200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$, in particular by the First Sylow Theorem we know that there exists a Sylow 5-subgroup of G and by the Third Sylow Theorem we know that the number of Sylow 5-subgroups of G divides 200 and is of the form $5 \cdot k + 1$ for $k \in \mathbb{N}$. Now:

$$
\begin{aligned}
1|200, \quad 6 \nmid 200, \quad 11 \nmid 200, \quad 16 \nmid 200, \quad 21 \nmid 200, \quad 26 \nmid 200,\\
31 \nmid 200, \quad 36 \nmid 200, \quad 41 \nmid 200, \quad 46 \nmid 200, \quad 51 \nmid 200,\\
56 \nmid 200, \quad 61 \nmid 200, \quad 66 \nmid 200, \quad 71 \nmid 200, \quad 76 \nmid 200,\\
81 \nmid 200, \quad 86 \nmid 200, \quad 91 \nmid 200, \quad 96 \nmid 200, \quad 101 \nmid 200,
\end{aligned}
$$

and obviously for $k > 20$ we have $(5 \cdot k + 1) \nmid 200$. Thus we have a unique Sylow 5-subgroup, which must be normal.

References

[1] T. W. Hungerford, *Algebra*.