Math 122: Algebra I, Fall 2023

Homework Assignment #6 (12 October 2023):
Cosets, Cauchy, etc.

Note on numbers and names

Below we present four theorems, labelled A, B, C and D. They are often numbered as "First isomorphism theorem", "Second…" and so on; however, there is no universal agreement on the numbering. Here we give some examples of the group isomorphism theorems in the literature. […]

—from Wikipedia's entry(*) on the isomorphism theorems, which proceeds to tabulate 11 different conventions, of which D&F's is the ninth.

* en.wikipedia.org/wiki/Isomorphism_theorems#Note_on_numbers_and_names (accessed 12 October 2023)

This problem set is due Wednesday, October 18 at midnight.

Another aspect of conjugation and normal subgroups:

1. [D&F 3.2 #5] Suppose H is a subgroup of G.
   i) Fix $g \in G$. Show that gHg^{-1} is a subgroup of G and that $|gHg^{-1}| = |H|$. (As usual gHg^{-1} means $\{ghg^{-1} \mid h \in H\}$.)
   ii) Deduce that if H has finite order n and H is the unique n-element subgroup of G then $H \trianglelefteq G$.

A classic application of Lagrange's Theorem to number theory:

2. [D&F 3.2 #16] Let p be a prime. Use Lagrange's Theorem in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$ to prove Fermat's Little Theorem: $a^p \equiv a \bmod p$ for all $a \in \mathbf{Z}$. [Warning: remember that the element $\bar{0}$ of $\mathbf{Z}/p\mathbf{Z}$ is not in $(\mathbf{Z}/p\mathbf{Z})^\times$.]

It is known that in fact $(\mathbf{Z}/p\mathbf{Z})$ is cyclic, but this result is somewhat harder and we probably won't cover it in Math 122. In particular if $l \mid p-1$ for some prime l then not only does $(\mathbf{Z}/p\mathbf{Z})^\times$ contain a subgroup of order l (which follows from Cauchy's theorem, see below) but this subgroup is unique, and the same is true also for composite factors l of $p-1$.

Cauchy proved in 1845 that if p is a prime factor of the order of a finite group G then G contains an element of order p. The following alternative proof (James H. McKay, *American Math. Monthly* **66** #2 (1959), p. 119) is surprisingly recent.

3–4. [D&F 3.2 #9] With G, p as above, let $\mathcal{S}$ denote the subset of G^p consisting of p-tuples $\vec{x} = (x_1, x_2, \ldots, x_p)$ whose product $x_1 x_2 \ldots x_p$ equals 1_G, and define $\sigma : G^p \to G^p$ by $\sigma((x_1, x_2, \ldots, x_{p-1}, x_p)) = (x_2, x_3, \ldots, x_p, x_1)$, so σ permutes the coordinates cyclically (whether or not $(x_1, \ldots, x_p) \in \mathcal{S}$).
   i) Prove that there is a well-defined action of $\mathbf{Z}/p\mathbf{Z}$ on G^p with $\overline{n} \cdot \vec{x} = \sigma^n(\vec{x})$ for all

$n \in \mathbf{Z}$ and $\vec{x} \in G^p$.

ii) The stabilizer of any $\vec{x} \in G^p$, being a subgroup of $\mathbf{Z}/p\mathbf{Z}$, is either $\{0\}$ or all of $\mathbf{Z}/p\mathbf{Z}$. Prove that the orbit of $\vec{x}$ has size p in the former case, and 1 in the latter, and that this latter case of stabilizer $\mathbf{Z}/p\mathbf{Z}$ occurs if and only if all the coordinates of $\vec{x}$ are equal, i.e. $\vec{x} = (x, x, \ldots, x)$ for some $x \in G$.

iii) Prove that σ, and thus the action of (i), takes $\mathcal{S}$ to $\mathcal{S}$.

iv) Prove that $\mathcal{S}$ has cardinality $|G|^{p-1}$, so in particular $|\mathcal{S}| \equiv 0 \bmod p$.

v) Deduce that the number of solutions $x \in G$ of $x^p = 1$ is a multiple of p. Conclude that the number of $x \in G$ of order p is congruent to $-1 \bmod p$, and in particular is nonzero, Q.E.D.

vi) Why is our proof of the $p = 2$ case of Cauchy's theorem (last problem of the first problem set) a special case of this argument?

Curiously, much the same argument applied to any group of size $a \neq 0 \bmod p$ yields another proof that $a^{p-1} \equiv 1 \bmod p$.

Applications of the isomorphism theorems:

5. [D&F 3.3 #3] Suppose $H \trianglelefteq G$ with $p := |G : H|$ prime. Prove that for any subgroup $K \leq G$, either $G = HK$ and $|K : (K \cap H)| = p$, or $K \leq H$.

6. [D&F 3.3 #8] Let p be a prime, and let G be the group $\{z \in \mathbf{C}^\times \mid \exists n \in \mathbf{N} : z^{p^n} = 1\}$ of p-power roots of 1 in $\mathbf{C}$ (cf. Exercise 18, §2.4 on p. 66). Prove that the map $z \mapsto z^p$ is a surjective homomorphism from G to G. Deduce that G is isomorphic to a proper quotient of itself (i.e. a quotient G/N where $N \neq \{1\}$).

7. [projective linear groups] For any field F and natural number $n \geq 1$, the nonzero scalar matrices $\{a\mathbf{1}_n \mid a \in F^\times\}$ commute with all of $\mathrm{GL}_n(F)$ and thus constitute a normal subgroup of $\mathrm{GL}_n(F)$, isomorphic with $F^\times$. (In fact it is known that this subgroup is the center of $\mathrm{GL}_n(F)$.) The quotient group is called the *projective general linear group* of order n, and denoted by $\mathrm{PGL}_n(F)$. The image of $\mathrm{SL}_n(F)$ under the quotient map $\mathrm{GL}_n(F) \to \mathrm{PGL}_n(F)$ is then naturally called the *projective special linear group* and denoted by $\mathrm{PSL}_n(F)$. Determine the index $|\mathrm{PGL}_n(\mathbf{R}) : \mathrm{PSL}_n(\mathbf{R})|$. When this index is not 1, determine the preimage of $\mathrm{PSL}_n(\mathbf{R})$ in $\mathrm{GL}_n(\mathbf{R})$. [NB the preimage won't be just $\mathrm{SL}_n(\mathbf{R})$, though it must contain $\mathrm{SL}_n(\mathbf{R})$.]

Why "projective"? Multiplication of matrices by column vectors gives an action of $\mathrm{GL}_n(F)$ on the vector space F^n; there isn't as obvious an action of $\mathrm{PGL}_n(F)$ on a vector space, but we shall see that it does act on a "projective space" $\mathbf{P}_{n-1}(F)$.