Math 71: Algebra **Fall 2022**

PSET 4 — 2022-11-11

Prof. Voight ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***Abstract Algebra*** by **David S. Dummit & Richard M. Foote**.

(b) ***Algebra*** by **Jacob K. Goldhaber & Gertrude Ehrlich**

Problems

1. Let $H := \{\epsilon, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subset S_4$.

(a) Show that H is a subgroup of S_4 and that H is isomorphic to $D_4 = \{1, r, s, sr\}$.

Let's name the components of H, such that $a = \epsilon$, $b = (1\,2)(3\,4)$, $c = (1\,3)(2\,4)$, and $d = (1\,4)(2\,3)$. For H to be a subgroup, it needs to:

(a) **Contain the identity element.**

This is trivial to prove, since ϵ is in H.

(b) **Be closed under inversion.**

All members of H aside from the identity have cycles of order 2. This makes each element its own inverse, since applying a two-cycle twice is the identity.

(c) **Be closed under composition.**

$$bc = (1\,2)(3\,4) \circ (1\,3)(2\,4) = (1\,4)(2\,3) = d$$

$$bd = (1\,2)(3\,4) \circ (1\,4)(2\,3) = (1\,3)(2\,4) = c$$

$$cb = (1\,3)(2\,4) \circ (1\,2)(3\,4) = (1\,4)(2\,3) = d$$

$$cd = (1\,3)(2\,4) \circ (1\,4)(2\,3) = (1\,2)(3\,4) = b$$

$$db = (1\,4)(2\,3) \circ (1\,2)(3\,4) = (1\,3)(2\,4) = c$$

$$dc = (1\,4)(2\,3) \circ (1\,3)(2\,4) = (1\,2)(3\,4) = b$$

Cayley Table:

	ϵ	b	c	d
ϵ	ϵ	b	c	d
b	b	ϵ	d	c
c	c	d	ϵ	b
d	d	c	b	ϵ

Now, we need to show that H is isomorphic to D_4. First, H and D_4 have the same order, since $|H| = |D_4| = 4$. Looking at H under composition, we see that every element is its own inverse, and $H = \{\epsilon, b, c, cb\}$ where $b = (1\,2)(3\,4)$, $c = (1\,3)(2\,4)$, and $bc = d = (1\,4)(2\,3)$.

Possible isomorphism:

$$\begin{aligned}\phi :\ & H \to D_4\\ & \epsilon \mapsto 1\\ & b \mapsto r\\ & c \mapsto s\end{aligned}$$

Then, $\phi(cb) = \phi(c) \cdot \phi(b) = s \cdot r = sr = \phi(d)$.

(b) What are the left cosets of H in S_4? How many are there, and how many elements are in each coset? Write each coset in the form xH for some $x \in S_4$.

$|H| = 4$ and $|S_4| = 4! = 24$. Therefore, H has a total of 5 left cosets in S_4. Each coset has 4 elements.

$$\epsilon \circ H = H = \{\epsilon, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

$$(1\,2) \circ H = \{(1\,2), (3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\}$$

$$(1\,3) \circ H = \{(1\,3), (1\,2\,3\,4), (2\,4), (1\,4\,3\,2)\}$$

$$(1\,4) \circ H = \{(1\,4), (1\,2\,4\,3), (1\,3\,4\,2), (2\,3)\}$$

$$(1\,2\,3) \circ H = \{(1\,2\,3), (1\,3\,4), (2\,4\,3), (1\,4\,2)\}$$

$$(1\,2\,4) \circ H = \{(1\,2\,4), (1\,4\,3), (1\,3\,2), (2\,3\,4)\}$$

(c) Show that $H \trianglelefteq S_4$ is normal. *[Hint: the cycle type is preserved under conjugation!]*

For H to be normal, It must hold that $hxh^{-1} = x$ for all $x \in S_4$ and $h \in H$. This condition is valid for all elements that have cycles of even order. Since all elements in H have cycles of order 2, this condition is valid for all elements in H, and H is normal.

(d) Show that $S_4/H \simeq S_3$. *[Hint: choose good representatives of the cosets.]*

Choosing the coset representatives $\epsilon,\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)$, We can interpret S_4/H as the set of permutations of S_4 that fix the element 4, i.e the stabilizers of 4. This is homomorphic to S_3 (if we disconsidered the element 4 altogether).

$$S_3 = \{\epsilon, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$$

$$S_4/H = \{\epsilon, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$$

The group H is denoted V_4 and called the *Klein four-group* (*Vierergruppe* in German, hence the label).

2. (DF 3.2.6–3.2.16)

(a) Prove that if $H, K \leq G$ are finite subgroups of a group G whose orders are relatively prime, then $H \cap K = \{1\}$.

Since H and K are finite subgroups of G, $H \cap K$ is also a finite subgroup of G, H, and K. By the Lagrange theorem, we know that $|H \cap K|$ divides $|H|$ and $|H \cap K|$ divides $|K|$. Since $|H|, |K|$ are relatively prime, $|H \cap K|$ must equal 1, and $H \cap K$ must be the trivial subgroup.

(b) Let $n \in \mathbb{Z}_{\geq 1}$. Use Lagrange's theorem applied to the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ to prove *Euler's theorem*: $a^{\phi(n)} \equiv 1 \pmod n$ for all $a \in \mathbb{Z}$ with $\mathbf{gcd}\ (a,\ n) = 1$. Conclude *Fermat's little theorem*: if p is a prime, then $a^{p-1} \equiv 1 \pmod p$ for all $a \in \mathbb{Z}$ with $\mathbf{gcd}\ (a,\ p) = 1$.

We know $|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \phi(n)$.
Let $a \in (\mathbb{Z}/n\mathbb{Z})$. Given $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, we know that $\mathbf{gcd}\ (a,\ n) = 1$.

If we consider the subgroup $\langle a \rangle$ generated by a, Lagrange's theorem tells us that its order must divide the order of $(\mathbb{Z}/n\mathbb{Z})^{\times}$, which is equal to $\phi(n)$.

Thus, $|a|$ divides $\phi(n)$, and we can write $\phi(n)$ as $x|a|$ for some $x \in \mathbb{Z}$. We also know that $a^{|a|} \equiv 1 \pmod n$. Using this, we can simplify $a^{\phi(n)}$:

$$\begin{aligned} a^{\phi(n)} &= a^{x|a|} \\ &= \left(a^{|a|}\right)^{x} \\ &= 1^{x} \pmod n \\ &= 1 \pmod n \end{aligned}$$

Suppose p is prime number, we have the special case that $\phi(p) = p - 1$, in which case $a^{p-1} \equiv 1 \pmod p$ for all numbers coprime with p — which is every other number in $\mathbb{Z}$ that is not p.

3. (DF 3.1.36)

Let G be a group.

(a) Show that the center $Z(G)$ is a normal subgroup of G.

Since $Z(G)$ is the center of G, every member $z \in Z(G)$ commutes with every other element of G. Let's pick one element $g \in G$ and write $gZ(G) = \{gz : z \in Z(G)\}$ and $Z(G)g = \{zg : z \in Z(G)\}$. Since every member of $Z(G)$ commutes with every member of G, $gZ(G) = Z(G)g$, and the subgroup $Z(G)$ is normal.

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian. *[Hint: if $G/Z(G) = \langle xZ(G) \rangle$, show that every element of G can be written in the form $x^r z$ for some $r \in \mathbb{Z}$ and some $z \in Z(G)$.]*

Given that $G/Z(G) = \langle xZ(G) \rangle$ for some $x \in G$. Since the left cosets of $Z(G)$ partition G, then every $g \in G$ can be written as a product of an element of $Z(G)$ and an element of $G/Z(G) = \langle xZ(G) \rangle$.

Taking $x^r z_1$ as the coset representative with $r \in \mathbb{Z}$, and the corresponding $z_2 \in Z(G)$ we can write $g = (x^r z_1)z_2$. However, since $Z(G)$ is a closed group, $z_1 z_2 = z \in Z(G)$, so $g = x^r z$ for some $z \in Z(G)$.

4. (sorta DF 3.1.40–41)

Let G be a group and $N \trianglelefteq G$ be a normal subgroup.

(a) Show that if G is abelian, then G/N is abelian.

We know each element of G/N is a coset gN for some $g \in G$. Let's take two such elements, xN and yN. Then we can see that $xN \cdot yN = yN \cdot xN$, and G/N is abelian:

$$\begin{aligned} xN \cdot yN &= xy \cdot N \\ &= yx \cdot N && \text{(Since } G \text{ is Abelian)} \\ &= yN \cdot xN \end{aligned}$$

(b) Show that G/N is abelian if and only if $aba^{-1}b^{-1} \in N$ for all $a, b \in G$. An element of G of the form $aba^{-1}b^{-1}$ is called a *commutator*.

If G/N is abelian, then G is abelian. Let's take two elements $a, b \in G$.

Suppose $aba^{-1}b^{-1} \notin N$. Then:

$$\begin{aligned} aba^{-1}b^{-1} &= a \cdot (ba^{-1}) \cdot b^{-1} \\ &= a \cdot (a^{-1}b) \cdot b^{-1} && \text{(Since } G \text{ is Abelian)} \\ &= aa^{-1} \cdot bb^{-1} \\ &= 1 \cdot 1 \\ &= 1 \in N \end{aligned}$$

This clearly contradicts the assumption that $aba^{-1}b^{-1} \notin N$. Therefore, if G/N is abelian, then $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

(c) Let $H := \langle aba^{-1}b^{-1} : a, b \in G \rangle$ be the subgroup of G generated by commutators, called the *commutator subgroup* of G. Show that $H \trianglelefteq G$ is a normal subgroup of G and that G/H is abelian. *[Hint: it is enough to check that the conjugate of a commutator is a commutator.]*

Let $h \in H$. Then $h = aba^{-1}b^{-1}$ for some $a, b \in G$. Let $g \in G$. Then:

$$
\begin{aligned}
ghg^{-1} &= g \cdot h \cdot g^{-1} \\
&= (h \cdot h^{-1}) \cdot g \cdot h \cdot g^{-1} \\
&= h \cdot (h^{-1}ghg^{-1})
\end{aligned}
$$

It is straightforward to see that $h^{-1}ghg^{-1}$ is a commutator. Since we took h from the commutator subgroup, the product of h and $h^{-1}ghg^{-1}$ must also be in the commutator subgroup. Therefore, $ghg^{-1} \in H$ for all $h \in H, g \in G$, and G/H is abelian.

5. (DF 3.2.13–14)

(a) Fix any labelling of the vertices of a square. Use this to identify D_8 as a subgroup of S_4 via its action on vertices. Prove that the elements of D_8 and $\langle(1\,2\,3)\rangle$ do not commute in S_4.

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Let's fix the edges of the square to be labelled $1, 2, 3, 4$ clockwise from the top-left corner. Then, we can identify D_8 as a subgroup of S_4 via its action on vertices.

$$D_8 := \{\epsilon, (1\,4\,3\,2), (1\,3)(2\,4), (1\,2\,3\,4), (1\,4)(2\,3), (2\,4), (1\,2)(3\,4), (1\,3)\}$$

(b) Prove that S_4 does not have a normal subgroup of order 8.

Suppose there exists a normal subgroup $N \trianglelefteq S_4$ of order 8. Then, the quotient group $S_4/N \cong C_3$ is abelian, which implies that N contains the commutator subgroup of S_4, which is A_4. So, $A_4 \in N$. However, $|A_4| = 12$ and $|N| = 8$, so $A_4 \notin N$. This contradiction shows that there cannot exist a normal subgroup of order 8 in S_4.