Math 71: Algebra	Fall 2022

PSET 3 — 3 november 2022

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. (sorta DF 1.7.18)

Let G be a group, let X be a set with an action by $G \circlearrowright X$.

(a) Prove that the relation $x \sim y$ if $x = g \cdot y$ for some $g \in G$ defines an equivalence relation on X. The set of equivalence classes are called the emphorbits of X under G.

(a) Reflexivity: $x \sim x$ for all $x \in X$.

We can show this trivially from the definition of group actions. The identity should map each element to itself.

$$e \cdot x = x \implies x \sim x$$

(b) Symmetry: $x \sim y$ implies $y \sim x$.

$$\begin{aligned} x \sim y &\iff x = g \cdot y \quad \text{for some } g \in G \\ &\implies y = g^{-1} \cdot x \quad \text{for some } g \in G \\ &\implies y \sim x \end{aligned}$$

(c) Transitivity: $x \sim y$ and $y \sim z$ implies $x \sim z$.

$$\begin{aligned} x \sim y &\iff x = g \cdot y \quad \text{for some } g \in G \\ y \sim z &\iff y = h \cdot z \quad \text{for some } h \in G \\ &\implies x = g \cdot y = g \cdot (h \cdot z) = (gh) \cdot z \quad \text{for some } g, h \in G \\ &\implies x \sim z \end{aligned}$$

(b) Show that the multiplicative group $G = \mathbb{R}^\times$ acts on the xy-plane $X = \mathbb{R}^2$ by $r \cdot (x, y) = (rx, y)$. What are the orbits of G acting on X? Compute the stabilizers of G on the points $(1, 1)$ and $(0, 0)$.

(a) The action is well defined by $r \cdot (x, y) = (rx, y)$.

$$1 \cdot (x, y) = (1 \cdot x, y) = (x, y)$$
$$r_1 r_2 \cdot (x, y) = (r_1 r_2 x, y) = r_1 \cdot (r_2 x, y) = r_1 \cdot (r_2 \cdot (x, y))$$

(b) The orbits for any point $(a, b) \in X$ are the lines $y = b$.

$$G \cdot X(a, b) = \{(ra, b) : r \in G\}$$

(c) The stabilizer of $(1, 1)$ and $(0, 0)$.

$$\begin{aligned} G_s(1, 1) &= \{r \in G : r \cdot (1, 1) = (1, 1)\} \\ &\implies r \cdot 1 = 1 \\ &\implies G_s(1, 1) = \{1\} \end{aligned}$$

$$\begin{aligned} G_s(0, 0) &= \{r \in G : r \cdot (0, 0) = (0, 0)\} \\ &\implies r \cdot 0 = 0 \\ &\implies G_s(0, 0) = R^\times \end{aligned}$$

2. (sorta DF 1.7.18)

Let F be a field, let $G = \mathrm{GL}_2(F)$, and let

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G : a, d \in F^\times,\, b \in F \right\}.$$

(a) Show that H is a subgroup of G, and show H is nonabelian whenever $\#F > 2$. What happens when $\#F = 2$ (so $F \simeq \mathbb{Z}/2\mathbb{Z}$)?

For H to be a subgroup of G, it must:

(a) contain the identity element $e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G$.

We see that $a = 1 \in F^\times$, $d = 1 \in F^\times$. and $b = 0 \in F$, so $e \in H$.

(b) be closed under multiplication.

Let $A, B \in H$. Suppose $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in H$ and $B = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in H$. Then $AB = \left(\begin{smallmatrix} ax & ay+bz \\ 0 & dz \end{smallmatrix}\right)$.

For AB to be in H, its elements must satisfy the conditions of H. Particularly:

(i) $a \in F^\times \ \wedge \ x \in F^\times \implies ax \in F^\times$.

(ii) $d \in F^\times \ \wedge \ z \in F^\times \implies dz \in F^\times$.

(iii) $ay + bz \in F$ since:

- $a \in F^\times \ \wedge \ y \in F^\times \implies ay \in F^\times \subset F$.
- $b \in F^\times \ \wedge \ z \in F^\times \implies bz \in F^\times \subset F$.
- $ay \in F \ \wedge \ bz \in F \implies ay + bz \in F$.

Therefore, we can infer that H is closed under multiplication.

(c) be closed under inversion.

Let $A \in H$, such that $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Then $A^{-1} = \left(\begin{smallmatrix} a^{-1} & -(ad)^{-1}b \\ 0 & d^{-1} \end{smallmatrix}\right)$.

We see that $A^{-1} \in H$ since its elements fit the specified domains. Particularly:

(i) $a \in F^\times \implies a^{-1} \in F^\times$.

(ii) $d \in F^\times \implies d^{-1} \in F^\times$.

(iii) $a \in F^\times \ \wedge \ d \in F \implies ad \in F^\times \implies (ad)^{-1} \in F^\times \subset F \implies -(ad)^{-1}b \in F$.

Therefore, we can infer that G is closed under inversion.

(b) Show that the map

$$\phi\colon H \to F^{\times}$$
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto a$$

is a surjective group homomorphism that is not an isomorphism.

To prove homomorphism:

(a) We need to prove that ϕ maps the identity element in H to the identity element in $F^{\times}$. Indeed, we see that:

$$e_H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \implies \phi(e) = 1 = e_{F^{\times}}$$

(b) We need to show that $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

Suppose that:

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in H \ \wedge \ B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in H$$

Then:

$$AB = \begin{pmatrix} ax & ay + bz \\ 0 & dz \end{pmatrix} \in H$$

and:

$$\phi(A) = a \in F^{\times}$$
$$\phi(B) = x \in F^{\times}$$
$$\phi(AB) = ax = \phi(A) \cdot \phi(B) \in F^{\times}$$

To prove isomorphism, we would have to prove that ϕ is bijective.

(a) It is trivial to prove that ϕ is surjective, since it maps a single matrix member $a \in F^{\times}$ of matrices in H back to $F^{\times}$, and the map does not change a.

(b) However, ϕ is not injective, since it multiple different matrices in H to the same element in $F^{\times}$. For example, we can take:

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in H \ \wedge \ B = \begin{pmatrix} a & x \\ 0 & y \end{pmatrix} \in H \quad : \quad b \neq x \wedge d \neq y$$

$$A \neq B$$

$$\phi(A) = \phi(B) = a$$

Therefore, ϕ cannot be an isomorphism because it is not injective.

3. (DF 1.3.1, sorta 1.3.7)

Let G be a group and let $A \subseteq G$ be a subset. For $g \in G$, write

$$gAg^{-1} := \{gag^{-1} : a \in A\}.$$

The *normalizer* of A in G is defined to be:

$$N_G(A) := \{g \in G : gAg^{-1} = A\}.$$

(a) Let $g \in G$. Show that the map

$$\begin{aligned} \phi_g \colon G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

is an isomorphism of groups. (We call an isomorphism from a group to itself an emphautomorphism.)

(a) ϕ_g is a homomorphism.

Let $x, y \in A, g \in G$. Then:

$$\begin{aligned} \phi_g(x) &= gxg^{-1} \\ \phi_g(y) &= gyg^{-1} \\ \phi_g(xy) &= gxyg^{-1} = (gxg^{-1}) \cdot (gyg^{-1}) = \phi_g(x) \cdot \phi_g(y) \end{aligned}$$

(b) ϕ_g is injective.

Suppose that $\phi_g(x) = \phi_g(y)$.

Then, $gxg^{-1} = gyg^{-1}$, which implies that $x = y$.

(c) ϕ_g is surjective.

Suppose $a \in A$ is some element acted on by ϕ_g, such that $a = \phi_g(a_0) = ga_0g^{-1}$ for some a_0, but $a \neq \phi_g(a_1)$ for all $a_1 \in A$.

Then:

$$\begin{aligned} ga_0g^{-1} \neq ga_1g^{-a} \quad &\forall \quad a_1 \in A \\ \implies a_0 \neq a_1 \quad &\forall \quad a_1 \in A \\ &\implies a_0 \notin A \end{aligned}$$

We see that any such element must be the result of ϕ_g acting on an element not contained in A, yet we defined ϕ_g to act on elements in A.

(b) Show that $N_G(A)$ is a subgroup of G that contains the centralizer $C_G(A)$. *[Hint: if $gAg^{-1} = A$ then $h(gAg^{-1})h^{-1} = hAh^{-1}$, we just took two equal sets and conjugated their elements by h.]*

(a) $N_G(A)$ is a subgroup of G.

Let $g, h \in N_G(A)$.

Then, $gAg^{-1} = A$ and $hAh^{-1} = A$.

Therefore, $ghAg^{-1}h^{-1} = A$ and $hAg^{-1}h^{-1} = A$.

Thus, $ghAh^{-1}g^{-1} = g(hAh^{-1})g^{-1} = gAg^{-1} = A$, which implies that $gh \in N_G(A)$.

Similarly, $hg \in N_G(A)$.

(b) $C_G(A) \subseteq N_G(A)$.

Let $g \in C_G(A)$.

Then, $gA = Ag$.

Therefore, $gAg^{-1} = Agg^{-1} = A$. Thus, $g \in N_G(A)$.

(c) Let $G = Q_8$ and let $A = \{\pm i\}$. Compute $C_G(A)$ and $N_G(A)$.

Cayley Table for Q_8:

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	i	1	$-k$	j
j	j	$-k$	-1	i	j	k	1	$-i$
k	k	j	$-i$	-1	k	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	$-i$	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	$-j$	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	$-k$	j	$-i$	-1

(a) $C_G(A) = \{\pm 1\}$.

$$gA = Ag$$

$$1 \cdot A = A \cdot 1$$

$$-1 \cdot A = A \cdot -1$$

All other elements do not satisfy this property. For instance, $i \cdot j = k$ but $j \cdot i = -k$.

(b) $N_G(A) = \{\pm 1, \pm i, \pm j, \pm k\}$.

$$gAg^{-1} = A$$

$$1^{-1} = 1$$
$$1 \cdot A \cdot 1 = A$$

$$-1^{-1} = -1$$
$$-1 \cdot A \cdot -1 = A$$

$$i^{-1} = -i$$
$$i \cdot j = k, k \cdot -j = i$$
$$-i \cdot j = -k, -k \cdot -j = -i$$

$$j^{-1} = -j$$
$$j \cdot k = i, -j \cdot i = k$$
$$-j \cdot k = -i, j \cdot -i = -k$$

$$k^{-1} = -k$$
$$k \cdot i = j, -k \cdot j = i$$
$$-k \cdot i = -j, k \cdot -j = i$$

(d) Show that if $H \leq G$ is a subgroup, then $H \leq N_G(H)$. *[Hint: use (a), with $G = H$.]*

Let $g \in H$.

Then, $ghg^{-1} = h$ for all $h \in H$ (by definition of the group operation).

However, this implies that $g \in N_G(H)$.

Therefore, it must hold that $H \leq N_G(H)$.

4. (DF 2.1.8)

Let $H, K \leq G$ be subgroups of a group G. Prove that the union $H \cup K$ is a subgroup if and only if $H \supseteq K$ or $K \subseteq H$. *[Hint: if there exists $h \in H$ with $h \notin K$, show that $K \subseteq H$ by consider hk for $k \in K$.]*

Suppose $H \nsubseteq K$ and $K \nsubseteq H$.

Then, there exists $h \in H, h \notin K$ and $k \in K, k \notin H$.

$$hk \in H \cup K \implies hk \in H \vee hk \in K$$

$$hk \in H \implies h^{-1} \cdot hk \in H \implies k \in H \qquad \text{(contradiction)}$$

$$hk \in K \implies hk \cdot k^{-1} \in K \implies h \in K \qquad \text{(contradiction)}$$

Therefore, for the union $H \cup K$ to be a subgroup, $H \subseteq K$ or $K \subseteq H$.

5. (DF 2.3.10)

(a) Let $G = \langle a \rangle$ be a cyclic group of order $n \in \mathbb{Z}_{\geq 1}$. For $k \in \mathbb{Z}$, show that a^k has order n/g where $g = \mathbf{gcd}\ (k,\ n)$. *[Hint: what is $\#\langle a^k \rangle$?]*

We can first observe that $\#\langle a \rangle = n \implies a^n = e$.

Suppose $m = \#\langle a^k \rangle$. Then $\left(a^k\right)^m = a^{km} = e$.

Since G is cyclic, this implies that $n \mid km$ (only powers of a that are multiples of n equal the identity).

$$\#\langle a \rangle = n \implies a^n = e$$

$$\#\langle a^k \rangle = m \implies \left(a^k\right)^m = a^{km} = e$$

Since a has order n, only powers of a that are equal to e are multiples of n. Let's write km as $km = pn, p \in \mathbb{Z}$.

Then:

$$a^{km} = a^{pn}$$

(b) What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements in $\langle \overline{30} \rangle$ and their orders.

We can first observe that $\mathbf{gcd}\ (30,\ 54) = 6$. Then:

$$o(\overline{30}) = \frac{54}{6} = 9$$

We can then write out all of the elements in $\langle \overline{30} \rangle$:

$$\langle \overline{30} \rangle = \{\overline{0}, \overline{30}, \overline{30}, \overline{6}, \overline{36}, \overline{312}, \overline{42}, \overline{18}, \overline{48}, \overline{24}\}$$

(c) For which values of $n \in \{8, 9, 10, 11, 12\}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$ a cyclic group?

$$
\begin{aligned}
(\mathbb{Z}/8\mathbb{Z})^\times &= \{1, 3, 5, 7\} \\
(\mathbb{Z}/9\mathbb{Z})^\times &= \{1, 2, 4, 5, 7, 8\} \\
(\mathbb{Z}/10\mathbb{Z})^\times &= \{1, 3, 7, 9\} \\
(\mathbb{Z}/11\mathbb{Z})^\times &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \\
(\mathbb{Z}/12\mathbb{Z})^\times &= \{1, 5, 7, 11\}
\end{aligned}
$$

Cyclic groups must have a generator g such that $\langle g \rangle = G$.

If we check the groups, we see:

(a) $(\mathbb{Z}/8\mathbb{Z})^\times$ lacks a generator, therefore it cannot be cyclic.

$$
\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle 3 \rangle &= \{3, 1\} \\
\langle 5 \rangle &= \{5, 1\} \\
\langle 7 \rangle &= \{7, 1\}
\end{aligned}
$$

(b) $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic, since $\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\}$.

(c) $(\mathbb{Z}/10\mathbb{Z})^\times$ is cyclic because $\langle 3 \rangle = \{3, 9, 7, 1\}$.

$$
\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle 3 \rangle &= \{3, 9, 7, 1\} \\
\langle 7 \rangle &= \{7, 9, 3, 1\} \\
\langle 9 \rangle &= \{9, 1\}
\end{aligned}
$$

(d) $(\mathbb{Z}/11\mathbb{Z})^\times$ is cyclic because $\langle 2 \rangle = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$.