Chris Hayduk
Math A4900
Homework 4
10/9/2020

1. **Generating groups**

(a) Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is isomorphic to Q_8.

Proof. We have the following relations for a,

$$\begin{aligned} a^2 &= a \cdot a \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} a^3 &= a \cdot a^2 \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} a^4 &= a \cdot a^3 \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I \end{aligned}$$

This gives us that $|a| = 4$. For b, we have,

$$\begin{aligned} b^2 &= b \cdot b \\ &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

and so,

$$\begin{aligned} b^4 &= (b^2)^2 \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I \end{aligned}$$

In addition, we have that $|b| = 4$ since 2 and 1 both divide 4, but $b^1, b^2 \neq I$.

Now we check the orders of ab and ba:

$$\begin{aligned} ab &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} (ab)^2 &= \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} (ab)^3 &= \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} (ab)^4 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

□

(b) A group is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$. For example, every finite group and every cyclic group is finitely generated.

Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.
[Show that if $H \leqslant \mathbb{Q}$ is generated by the finite set A, then $H \leqslant \langle 1/k \rangle$ where k is the product of all the denominators that appear in A. Now, what do you know about subgroups of cyclic groups?]

Proof. Let H be a finitely generated subgroup of $\mathbb{Q}$. That is, there is a finite set $A \subset \mathbb{Q}$ such that $H = \langle A \rangle$. □

2. **Quotient groups**

(a) Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a+ib) = a^2 + b^2 = |a+ib|^2$.
[Note: Remember that you know about polar coordinates for complex numbers. Namely, $re^{ix} = r\cos(x) + ir\sin(x)$ and $a + bi = |a+ib|e^{i\arctan(b/a)}$.]

(i) Prove φ is a homomorphism, and compute its image.

Proof. Let $a, b \in \mathbb{C}$. Then we can write $a = a_1 + ia_2$ and $b = b_1 + ib_2$ where $a_1, a_2, b_1, b_2 \in \mathbb{R}$. Moreover, we have that,

$$\begin{aligned} a \cdot b &= (a_1 + ia_2) \cdot (b_1 + ib_2) \\ &= a_1b_1 + ia_1b_2 + ia_2b_1 - a_2b_2 \\ &= a_1b_1 - a_2b_2 + i(a_1b_2 + a_2b_1) \end{aligned}$$

This gives us,

$$\begin{aligned} \varphi(ab) &= (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 - 2a_1b_1a_2b_2 + a_2^2b_2^2 + a_1^2b_2^2 + 2a_1b_2a_2b_1 + a_2^2b_1^2 \\ &= a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2 \end{aligned}$$

Now let us check $\varphi(a)\varphi(b)$,

$$\begin{aligned} \varphi(a) \cdot \varphi(b) &= (a_1^2 + a_2^2) \cdot (b_1^2 + b_2^2) \\ &= a_1^2b_1^2 + a_1^2b_2^2 + a_2^2b_1^2 + a_2^2b_2^2 \\ &= \varphi(ab) \end{aligned}$$

So we have that $\varphi(a) \cdot \varphi(b) = \varphi(ab)$ for any $a, b \in \mathbb{C}$, as required.

The image of φ is $\{x \in \mathbb{R} : x \geqslant 0\}$. This true because $a^2 + b^2 \geqslant 0$ for any choice of $a, b \in \mathbb{R}$. In addition, if we fix $b = 0$ and let a range over $\mathbb{R}$, we have that φ maps to all the positive real numbers. Hence, the image of φ as described above. □

(ii) Describe the fibers geometrically (as subsets of the complex plane). [Draw some pictures!]

Answer. Observe that, for any $x \in \mathbb{R}_{\geqslant 0}$, the pre-image of x under φ is the set $\{c = a + ib \in \mathbb{C} : a^2 + b^2 = x\}$. Observe that $a, b \in \mathbb{R}$ and $x \in \mathbb{R}_{\geqslant 0}$. Hence, $a^2 + b^2 = x$ is precisely the equation for a circle in $\mathbb{R}^2$ with radius x. We can map these circles onto $\mathbb{C}$ by mapping b to ib. Hence, the fibers of φ are represented by circles in the complex plane, where the radius of each circle is the real number x that these complex numbers map to.

. . . .

(iii) Express the non-empty fibers algebraically as left cosets of the kernel.

Answer. Observe that,

$$K = \ker(\varphi) = \{c = a + ib \in \mathbb{C} : a^2 + b^2 = 1\}$$

Now fix $c_1 = a_1 + ib_1 \in \mathbb{C}$ and $c_2 = a_2 + ib_2 \in K$. Then we have,

$$c_1 \cdot c_2 = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$$

We also have that,

$$\begin{aligned}\varphi(c_1c_2) &= \varphi(c_1) \cdot \varphi(c_2)\\ &= \varphi(c_1) \cdot 1\\ &= \varphi(c_1)\\ &= a_1^2 + b_1^2\end{aligned}$$

So for any $c \in \mathbb{C}$, we have that cK maps every element of K into an element in the pre-image of $\varphi(c)$

. . . .

(b) Let $m, d \in \mathbb{Z}_{\geqslant 2}$ and let $n = md$. Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by $\bar{a} \to \bar{a}$.

(i) Show that φ is a well-defined, surjective homomorphism.

Proof. Observe that $n > m$. Hence, we will first check the case where $\bar{a} < m$. Consider $\varphi(\bar{a})$. Since $\bar{a} < m$, we have that $\bar{a} \equiv \bar{a} \mod m$ by definition. Thus, we have $\bar{a} = \varphi(\bar{a})$ and so φ is defined here. In addition, this actually gives us surjectivity. Take $\bar{0}, \bar{1}, \cdots \overline{m-1} \in \mathbb{Z}/n\mathbb{Z}$. Then we have $\varphi(\bar{0}) = \bar{0}, \varphi(\bar{1}) = \bar{1}, \cdots, \varphi(\overline{m-1}) = \overline{m-1}$. These are precisely all the equivalence classes in $\mathbb{Z}/m\mathbb{Z}$, so φ is surjective.

Now consider $\bar{a} \geqslant m$. By the definition of equivalence classes in $\mathbb{Z}/m\mathbb{Z}$, we have $\bar{b} \in \bar{a}$ with $b < a$. Hence, $\varphi(\bar{a}) = \bar{a}$ is well-defined here as well. As a result, we have that φ is well-defined and surjective. Now we need to show that φ is a homomorphism.

Let $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$. Then we have,

$$\bar{a} + \bar{b} = \overline{a+b} \in \mathbb{Z}/n\mathbb{Z}$$

Thus, we have,

$$\begin{aligned}\varphi(\bar{a} + \bar{b}) &= \bar{a} + \bar{b}\\ &= \overline{a+b}\\ &= \varphi(\overline{a+b})\end{aligned}$$

Since $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ were arbitrary, we have that φ is a homomorphism. $\square$

(ii) Show that $\ker(\varphi) \cong \mathbb{Z}/d\mathbb{Z}$. Describe the fibers, and express them as left cosets of the kernel.
[Note: since $\mathbb{Z}/n\mathbb{Z}$ is an additive group, the cosets will look like $x + K$, not xK.
Don't know where to start? Do some examples! Draw some pictures!]

Proof. We have that,

$$K = \ker(\varphi) = \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} : \bar{x} = \bar{0}\}$$

We have that $\varphi(\bar{0}) = \bar{0}$ by definition, so $\bar{0} \in K$. Now observe that, for any $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ (with $x \neq 0$), $\varphi(\bar{x}) \in K$ if and only if $m|x$. We know $n = md$ where $d \geqslant 2$, so the equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ are $\bar{0}, \bar{1}, \cdots, \overline{md-1}$. Thus, we have that the possible multiples of m in $\mathbb{Z}/n\mathbb{Z}$ are $\overline{m}, \overline{2m}, \cdots, \overline{m(d-1)}$. Hence, we now have that,

$$K = ker(\varphi) = \{\overline{0m} = \bar{0}, \overline{m}, \overline{2m}, \cdots, \overline{m(d-1)}\}$$

Now define $\varphi_1 : K \to \mathbb{Z}/d\mathbb{Z}$ by the $\varphi(\overline{xm}) = \bar{x}$. Since every element in the set K as defined above has an associated x, this function is well-defined. Now let $\bar{a} = \overline{x_1 m}, b = \overline{x_2 m} \in K$. Then,

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{x_1 m + x_2 m} \\ &= \overline{m(x_1 + x_2} \end{aligned}$$

And so we have that,

$$\begin{aligned} \varphi_1(\overline{a+b}) &= \overline{m(x_1 + x_2)} \\ &= \overline{x_1 m} + \overline{x_2 m} \\ &= \varphi_1(\bar{a}) + \varphi_1(\bar{b}) \end{aligned}$$

Thus, φ_1 is a homomorphism. We have that φ_1 is surjective because the equivalence classes for $\mathbb{Z}/d\mathbb{Z}$ are $\bar{0}, \bar{1}, \cdots, d \bar{-} 1$, and all of these numbers appear as a multiple of m in K. Now let us show injectivity. Let $\bar{a} = \overline{x_1 m}, \bar{b} = \overline{x_2 m} \in K$ with $a \neq b$ and suppose $\varphi_1(\bar{a}) = \varphi_1(\bar{b})$. Then we have,

$$\overline{x_1} = \overline{x_2}$$

Since every $\overline{x_1 m}, \overline{x_2 m} \in K$ are distinct, we have that $\overline{x_1} = \overline{x_2}$ if and only if $\overline{x_1 m} = \overline{x_2 m}$. Hence, φ_1 is injective and is thus an isomorphism. As a result, we have that $\ker(\varphi) \cong \mathbb{Z}/d\mathbb{Z}$, as required. □

(iii) Show that $(\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/d\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$.

Proof. We know that $(\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/d\mathbb{Z})$ is the group whose elements are the fibers of φ with the following group operation: if X is the fiber of $\overline{a}$ and Y is the fiber above b, then the sum of X and Y is defined to be the fiber above $\overline{a+b}$ □

(c) Show $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$, and describe $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$.
[Hint: What homomorphism out of $\mathrm{GL}_n(F)$ is $\mathrm{SL}_n(F)$ the kernel of? Use the 1st isomorphism thm.]

Answer. Note that,

$$\mathrm{GL}_n(F) = \{A : A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}$$

where F is a field. We also have,

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) : \det(A) = 1\}$$

. . . .

(d) If $N \trianglelefteq G$, we know G/N is a group. Is it necessarily true that G/N is isomorphic to a subgroup of G? If yes, prove it; if no, give a counterexample.

3. **Normal subgroups**

(a) Show that if $N \trianglelefteq G$ and $H \leqslant G$, then $H \cap N \trianglelefteq H$. Give an example showing that it's not necessarily true that $H \cap N \trianglelefteq G$.

Proof. Let $N \trianglelefteq G$ and let $H \leqslant G$. Now consider $H \cap N$. Since $N \trianglelefteq G$ and $H \leqslant G$, we have $H \cap N \subset G$. In addition, we have that $1 \in H \cap N$ since 1 is in every subgroup and N, H are both subgroups. Hence, $H \cap N \neq \varnothing$.

Now fix $x, y \in H \cap N$. We have that $x, y \in H, N$ by definition. Since H, N are both groups, then $y^{-1} \in H, N$ by closure under inverses of subgroups and $xy^{-1} \in H, N$ by closure under multiplication of subgroups. Now,, since $xy^{-1} \in H, N$, we have $xy^{-1} \in H \cap N$ by the definition of intersections. Hence, $H \cap N$ satisfies the subgroup criterion and thus $H \cap N \leqslant G$.

Now we need to show that $H \cap N \trianglelefteq G$ $\square$

(b) Let N be a finite subgroup of G and assume $N = \langle S \rangle$ for some subset $S \subseteq G$. Prove that $g \in N_G(N)$ if and only if $gSg^{-1} \subseteq N$.