Abstract Algebra - Homework 1

Simon Gustafsson

Problem 1

Let $k = \mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. We define $\mathrm{GL}_2(k)$ as the group of all invertible 2×2 matrices with entries in the field k. In other words,

$$\mathrm{GL}_2(k) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \;\middle|\; ad - bc \neq 0 \right\}.$$

$\mathrm{GL}_2(k)$ Forms a Group

Let $A, B \in \mathrm{GL}_2(k)$. Then the product AB is defined as:

$$AB = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix},$$

where all entries involve only addition and multiplication of elements in k. Since k is a field, it is closed under addition and multiplication, so all entries of AB lie in k. Furthermore, $\det(AB) = \det(A)\det(B) \neq 0$, so $AB \in \mathrm{GL}_2(k)$. Thus, $\mathrm{GL}_2(k)$ is closed under matrix multiplication.

Since matrix multiplication is associative, the operation on $\mathrm{GL}_2(k)$ is associative.

The identity element in $\mathrm{GL}_2(k)$ is the identity matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For any $A \in \mathrm{GL}_2(k)$, we have $AI = IA = A$, and since the entries 1 and 0 are in k, we conclude $I \in \mathrm{GL}_2(k)$.

Since every element of $\mathrm{GL}_2(k)$ is invertible by definition, the inverse of

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$$

is given by:

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Since $a, b, c, d \in k$, and $\det(A) = ad - bc \neq 0$, we have $\frac{1}{\det(A)} \in k$, because k is a field. As k is closed under addition, subtraction, and multiplication, all entries of A^{-1} lie in k. Hence, $A^{-1} \in \mathrm{GL}_2(k)$.

Therefore, $\mathrm{GL}_2(k)$ satisfies the group axioms under matrix multiplication and is a group.

The Center of $\mathrm{GL}_2(k)$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$. Suppose $A \in Z(\mathrm{GL}_2(k))$. Then for all $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathrm{GL}_2(k)$, we must have

$$AB = BA.$$

Compute both sides:

$$AB = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}, \quad BA = \begin{pmatrix} ea + fc & eb + fd \\ ga + hc & gb + hd \end{pmatrix}.$$

For these to be equal for all $e, f, g, h \in k$, compare the corresponding entries:

$$\begin{aligned} ae + bg = ea + fc &\quad \Rightarrow \quad b = c = 0 \\ af + bh = eb + fd &\quad \Rightarrow \quad a = d, \text{ using } b = 0 \\ ce + dg = ga + hc &\quad \Rightarrow \quad c = b = 0 \\ cf + dh = gb + hd &\quad \Rightarrow \quad d = a \end{aligned}$$

Hence, A must be of the form:

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I,$$

where $\lambda \in k^\times = k \setminus \{0\}$ (since A must be invertible). Thus,

$$Z(\mathrm{GL}_2(\mathbb{F}_7)) = \left\{ \lambda I \mid \lambda \in k^\times \right\}.$$

This center consists of 6 elements and forms an abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$.

Group Action on $\mathbb{P}^1(k)$

We define the projective line over k as $\mathbb{P}^1(k) = k \cup \{\infty\}$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$. Then the action of $\mathrm{GL}_2(k)$ on $\mathbb{P}^1(k)$ is given by the formula:

$$A \cdot z = \begin{cases} \dfrac{az+b}{cz+d}, & \text{if } z \in k \text{ and } cz+d \neq 0, \\ \infty, & \text{if } z \in k \text{ and } cz+d = 0, \\ \dfrac{a}{c}, & \text{if } z = \infty \text{ and } c \neq 0, \\ \infty, & \text{if } z = \infty \text{ and } c = 0. \end{cases}$$

We verify that this defines a group action.

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then for all $z \in \mathbb{P}^1(k)$,

$$I \cdot z = \frac{1 \cdot z + 0}{0 \cdot z + 1} = \frac{z}{1} = z, \quad \text{and} \quad I \cdot \infty = \frac{1}{0} := \infty.$$

So the identity acts as the identity function.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be in $\mathrm{GL}_2(k)$, and let $z \in \mathbb{P}^1(k)$. Then:

$$B \cdot z = \frac{ez+f}{gz+h}, \quad \text{and} \quad A \cdot (B \cdot z) = \frac{a \cdot \left(\frac{ez+f}{gz+h}\right) + b}{c \cdot \left(\frac{ez+f}{gz+h}\right) + d}.$$

Simplifying this gives:

$$A \cdot (B \cdot z) = \frac{(aez + af + bgz + bh)}{(cez + cf + dgz + dh)} = \frac{(ae+bg)z + (af+bh)}{(ce+dg)z + (cf+dh)},$$

which is the action of the product matrix AB on z:

$$(AB) \cdot z.$$

Thus, the compatibility condition holds.

Therefore, the formula defines a group action of $\mathrm{GL}_2(k)$ on $\mathbb{P}^1(k)$.

Transitivity and the Stabilizer of 0

Let $z \in \mathbb{P}^1(k)$ be arbitrary. We want to find a matrix $A \in \mathrm{GL}_2(k)$ such that $A \cdot 0 = z$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k).$$

Then the action on 0 is given by

$$A \cdot 0 = \frac{b}{d},$$

provided $d \neq 0$. For any $z \in k$, we can take $b = z$ and $d = 1$, with $a \in k^\times$, $c \in k$ arbitrary, such that $\det(A) = ad - bc \neq 0$.

To obtain ∞, we require $d = 0$, in which case the formula becomes

$$A \cdot 0 = \frac{b}{d} = \infty,$$

provided $b \neq 0$. We can choose $a, c \in k$ arbitrarily so that $\det(A) = -bc \neq 0$, ensuring $A \in \mathrm{GL}_2(k)$.

Hence, for any $z \in \mathbb{P}^1(k)$, there exists a matrix $A \in \mathrm{GL}_2(k)$ such that $A \cdot 0 = z$. Therefore, the action is transitive.

We require $A \cdot 0 = 0$, so $\frac{b}{d} = 0 \Rightarrow b = 0$. Therefore, the stabilizer of 0 is the set of all invertible lower triangular matrices:

$$B = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k) \;\middle|\; a, d \in k^\times,\ c \in k \right\}.$$

Kernel of the Action

The kernel of the action can be defined as follows,

$$\ker = \left\{ A \in \mathrm{GL}_2(k) \mid A \cdot z = z \text{ for all } z \in \mathbb{P}^1(k) \right\}.$$

Then, for all $z \in k$,

$$\begin{aligned} A \cdot z = \frac{az + b}{cz + d} &= z \\ &\implies az + b = z(cz + d) = cz^2 + dz \\ &\implies cz^2 + (d - a)z - b = 0 \\ &\implies \quad c = 0, \quad d = a, \quad b = 0. \end{aligned}$$

Therefore,

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI, \quad \text{with } a \in k^\times.$$

These are exactly the scalar matrices which form the center. Hence, the kernel of the action is the center of $\mathrm{GL}_2(k)$.

Intersection of Conjugates of the Stabilizer

Let $B \subseteq \mathrm{GL}_2(k)$ be the stabilizer of $0 \in \mathbb{P}^1(k)$. We claim that

$$\bigcap_{g \in \mathrm{GL}_2(k)} gBg^{-1} = Z(\mathrm{GL}_2(k)).$$

This follows from the general fact that, if a group G acts transitively on a set X, then the intersection of all conjugates of the stabilizer G_x is equal to the kernel of the associated homomorphism:

$$\bigcap_{g \in G} gG_xg^{-1} = \ker(G \to \mathrm{Sym}(X)).$$

In our case, $G = \mathrm{GL}_2(k)$, $X = \mathbb{P}^1(k)$. We have already shown that the action is transitive, and that the kernel of the action is the center:

$$\ker = Z(\mathrm{GL}_2(k)).$$

Therefore,

$$\bigcap_{g \in \mathrm{GL}_2(k)} gBg^{-1} = Z(\mathrm{GL}_2(k)).$$

Problem 2

Let X be the set of all k-element subsets of $\{1, \ldots, n\}$, and let S_n act on X by

$$\sigma \cdot E := \{\sigma(e) \mid e \in E\}.$$

Fix the subset $A = \{1, \ldots, k\} \in X$. The stabilizer of A consists of all permutations in S_n that fix A setwise. These are exactly the permutations that act as an element of S_k on the set $\{1, \ldots, k\}$, and as an element of S_{n-k} on its complement $\{k+1, \ldots, n\}$, independently. Thus,

$$\mathrm{Stab}_{S_n}(A) \cong S_k \times S_{n-k}.$$

By the Orbit-Stabilizer Theorem, the number of k-element subsets is

$$|X| = [S_n : \mathrm{Stab}_{S_n}(A)] = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Problem 3

Group action

Let G be a finite group and $H \subset G$ a subgroup. Define a map

$$\phi : H \times (G/H) \to G/H, \quad (h, gH) \mapsto (hg)H.$$

To verify that ϕ defines a group action, we check the two axioms. For all $gH \in G/H$,

$$e \cdot gH = (eg)H = gH.$$

For all $h_1, h_2 \in H$ and $gH \in G/H$,

$$h_1 \cdot (h_2 \cdot gH) = h_1 \cdot (h_2 gH) = (h_1 h_2 g)H = ((h_1 h_2) \cdot gH).$$

Hence, the identity and compatibility axioms are satisfied. Since we are viewing G/H purely as a set of left cosets (not as a quotient group), this confirms that ϕ defines a group action of H on the set G/H.

Trivial action implies normality

Suppose ϕ is trivial. That means for all $h \in H$ and $gH \in G/H$, we have:

$$\phi(h, gH) = gH \quad \Rightarrow \quad (hg)H = gH.$$

This implies:

$$hg \in gH \quad \Rightarrow \quad g^{-1}hg \in H \quad \text{for all } h \in H, g \in G.$$

Therefore, H is closed under conjugation by elements of G, i.e., $gHg^{-1} \subseteq H$. Since $g \in G$ was arbitrary, it follows that H is a normal subgroup of G.

The action is not transitive

Assume $[G : H] = p$, where p is the smallest prime dividing $|G|$.

Suppose that the action is transitive. Then the orbit of any element $gH \in G/H$ under the action of H is the entire set G/H, which has p elements.

But the size of any orbit under a group action divides the order of the acting group and in this case, $|H| = |G|/p$.

Therefore, the size of the orbit must divide $|H| = |G|/p$, but it is equal to p. Since p is the smallest prime dividing $|G|$, it does not divide $|G|/p$, and thus does not divide $|H|$.

This is a contradiction. Hence, the action cannot be transitive.

Class equation and normality

From the theory of group actions, we have the orbit decomposition:

$$|G/H| = \sum_{i=1}^{r} |\mathcal{O}_i|,$$

where $\mathcal{O}_i$ are the distinct orbits of the action of H on the set G/H.

Since $|G/H| = p$, a prime number, the possible orbit decompositions are very limited. One possibility is that there is a single orbit of size p, but this would imply that the action is transitive, which we ruled out in the previous section. Another possibility is that there is one orbit of size 1 and one of size $p - 1$, but the size of each orbit must divide $|H| = |G|/p$. Since p is the smallest prime dividing $|G|$, it does not divide $|G|/p$, and therefore cannot divide any orbit size greater than 1.

The only remaining possibility is that all orbits have size 1. That means:

$$(hg)H = gH \quad \forall h \in H,\, gH \in G/H,$$

which implies $hg \in gH \Rightarrow g^{-1}hg \in H$, i.e., H is invariant under conjugation by all $g \in G$. Therefore, $H \trianglelefteq G$.