

# Abstract Algebra - Homework 1

Simon Gustafsson

## Problem 1

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

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

(1) Let  $A, B \in \text{GL}_2(k)$ . 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  $AB \in \text{GL}_2(k)$ . Thus,  $\text{GL}_2(k)$  is closed under matrix multiplication.

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

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

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

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

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

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

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,  $A^{-1} \in \text{GL}_2(k)$ .

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

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

$$AB = BA.$$

Where,

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

For these to be equal  $\forall e, f, g, h \in k$ , the corresponding entries must be;

$$\begin{aligned} ae + bg = ea + fc &\implies bg = fc \implies b = c = 0, \\ af + bh = fd &\implies af = fd \implies a = d. \end{aligned}$$

Hence,  $A$  must be of the form:

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

where  $\lambda \in k^\times = k \setminus \{0\}$  as a consequence of the fact that  $A$  is invertible. Thus,

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

(2) For the identity matrix  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  we have

$$I \cdot z = \frac{1 \cdot z + 0}{0 \cdot z + 1} = z, \quad \forall z \in k \quad I \cdot \infty = \infty.$$

Thus  $I$  acts as the identity on  $\mathbb{P}^1(k)$ .

For  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \text{GL}_2(k)$ ,

$$\begin{aligned} A \cdot (B \cdot z) &= \frac{a \frac{ez+f}{gz+h} + b}{c \frac{ez+f}{gz+h} + d} \\ &= \frac{(ae + bg)z + (af + bh)}{(ce + dg)z + (cf + dh)} \\ &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \cdot z \\ &= (AB) \cdot z \end{aligned}$$

For  $z = \infty$  we have  $B \cdot \infty = e/g$  if  $g \neq 0$  and  $\infty$  if  $g = 0$ ; in either case the same calculation gives  $A \cdot (B \cdot \infty) = (AB) \cdot \infty$ . Thus  $A \cdot (B \cdot z) = (AB) \cdot z, \forall z \in \mathbb{P}^1(k)$ . This verifies that the formula defines a group action of  $\text{GL}_2(k)$  on  $\mathbb{P}^1(k)$ .

- (3) Let  $z \in \mathbb{P}^1(k)$  be arbitrary and let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(k)$ . 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  $\infty$ , 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  $A \in \text{GL}_2(k)$ .

Hence, for any  $z \in \mathbb{P}^1(k)$ , there exists a matrix  $A \in \text{GL}_2(k)$  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:

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

(4) The kernel of the action can be defined as follows,

$$\ker = \{A \in \mathrm{GL}_2(k) \mid A \cdot z = z, \forall z \in \mathbb{P}^1(k)\}.$$

Then,  $\forall z \in k$ ,

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

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  $\mathrm{GL}_2(k)$ .

(5) 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:

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

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

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

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

Fix the subset  $A = \{1, \dots, k\} \in X$ . 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  $\{1, \dots, k\}$ , and as an element of  $S_{n-k}$  on its complement  $\{k+1, \dots, n\}$ , independently. Thus,

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

- (2) By the Orbit-Stabiliser Theorem and the isomorphism found in previous section,

$$|X| = \frac{|S_n|}{|\text{Stab}_{S_n}(A)|} = \frac{n!}{|S_k| \cdot |S_{n-k}|} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

## Problem 3

- (1) To verify that  $\phi$  defines a group action, we check the two axioms. For all  $gH \in G/H$ ,

$$\phi(e, gH) = (eg)H = gH.$$

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

$$\phi(h_1, \phi(h_2, gH)) = \phi(h_1, (h_2g)H) = (h_1h_2g)H = \phi(h_1h_2, gH).$$

Hence, the identity and compatibility axioms are satisfied. This confirms that  $\phi$  defines a group action of  $H$  on the set  $G/H$ .

- (2) Suppose  $\phi$  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  $G$ .

- (3) 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.

- (4) 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,  $H \trianglelefteq G$ .

## Problem 4

- (1) By definition,  $V_4$  contains the identity element. To show that  $V_4$  is normal in  $S_4$ , we verify that it is invariant under conjugation. For any  $\sigma \in S_4$  and  $v \in V_4$ , we have  $\sigma v \sigma^{-1}$  is again a product of two disjoint transpositions. Since there are exactly three such elements in  $S_4$ , and they form a conjugacy class, it follows that conjugation by any  $\sigma \in S_4$  sends elements of  $V_4$  to other elements in  $V_4$ .

Hence,  $V_4$  is closed under conjugation, and we conclude that  $V_4 \trianglelefteq S_4$ .

- (2) Consider the subgroup  $H = \langle (12), (123) \rangle \subset S_4$ . This subgroup permutes the elements  $\{1, 2, 3\}$  and fixes 4, so it is isomorphic to  $S_3$ . We identify  $S_3$  with this subgroup  $H$ .

We define the map

$$f : S_3 \rightarrow S_4/V_4, \quad f(\sigma) = \sigma V_4.$$

First, it is well-defined: each  $\sigma \in S_3$  is interpreted as an element of  $H \subset S_4$ , and the left coset  $\sigma V_4$  is a valid element of the quotient  $S_4/V_4$ . The map is injective because  $H \cap V_4 = \{\text{Id}\}$ , so no two distinct elements of  $H$  lie in the same coset. It is surjective since  $H$  has 6 elements and  $|S_4/V_4| = 6$ , meaning the image of  $f$  exhausts all cosets. Finally,  $f$  is a homomorphism: for all  $\sigma_1, \sigma_2 \in S_3$ , we have

$$f(\sigma_1 \sigma_2) = \sigma_1 \sigma_2 V_4 = \sigma_1 V_4 \cdot \sigma_2 V_4 = f(\sigma_1) f(\sigma_2).$$

Thus,  $f$  is a bijective homomorphism and therefore an isomorphism.

- (3) From group theory, the normal subgroups of  $S_4$  are:

$$\{\text{Id}\}, \quad V_4, \quad A_4, \quad S_4.$$

Here  $A_4$  denotes the alternating group on four letters, the set of all even permutations, so it is normal in  $S_4$ . Moreover, because each element of  $V_4$  is a product of two transpositions (an even permutation), we have  $V_4 \subset A_4$ . The subgroups that contain  $V_4$  are  $V_4, A_4, S_4$ . These are all normal in  $S_4$ , and there are no other normal subgroups strictly between  $V_4$  and  $S_4$ . Hence, the normal subgroups of  $S_4$  containing  $V_4$  are  $V_4, A_4, S_4$ .

## Problem 5

- (1) Since  $5 < 7$  and  $5 \nmid (7-1) = 6$ , the  $pq$ -order theorem implies that every group of order  $pq$  with those divisibility conditions is cyclic. Hence

$$G \cong \mathbb{Z}_{35}.$$

For a cyclic domain, a homomorphism is completely determined by the image of a generator  $g \in G$ . Suppose

$$\varphi : G \longrightarrow S_3, \quad \varphi(g) = x.$$

Then  $\text{ord}(x)$  must divide  $\text{ord}(g) = 35$ .

The possible element orders in  $S_3$  are 1, 2, 3, and among these only 1 divides 35. Therefore  $x$  must be the identity permutation; consequently  $\varphi$  sends every element of  $G$  to the identity in  $S_3$ . This is the trivial homomorphism, and no other homomorphism can exist.

- (2) An action of  $G$  on the set  $E = \{1, 2, 3\}$  is equivalent to a group homomorphism

$$\rho : G \longrightarrow \text{Sym}(E) = S_3.$$

In the previous section we proved that, for a group  $G$  of order 35, the only homomorphism  $G \rightarrow S_3$  is the trivial one.

Hence there is exactly 1 action of  $G$  on  $E$ , namely the trivial action  $g \cdot x = x$  for all  $g \in G$  and  $x \in E$ .

- (3) Because  $|E| = 3$ , the possible orbit decompositions are 3,  $2 + 1$ , or  $1 + 1 + 1$ . A single orbit of size 3 contradicts non-transitivity, while three singleton orbits give the trivial action. Hence  $E$  must split into one orbit of size 2 and one of size 1.

Let  $y$  lie in the two-element orbit and  $x$  in the singleton orbit. By the Orbit-Stabiliser Theorem,

$$|G| = |G \cdot y| |G_y| = 2 |G_y|, \quad |G| = |G \cdot x| |G_x| = 1 \cdot |G_x|.$$

Thus

$$|G_x| = |G|, \quad |G_y| = \frac{|G|}{2}.$$



Because  $|G|$  is even,  $|G_y|$  is an integer, and the stabiliser of  $y$  has index 2 in  $G$ . The action is genuinely non-trivial, because the two-element orbit is not fixed point-wise. There exists some  $g \in G$  with  $g \cdot y \neq y$ .

Therefore the only non-trivial, non-transitive action has two orbits of sizes 2 and 1. The singleton orbit is fixed point-wise, while the stabiliser of each point in the two-element orbit has index 2 in  $G$ .

- (4) Suppose  $G$  has odd order and acts on  $E = \{1, 2, 3\}$ . If the action were non-transitive and non-trivial, previous section implies that  $E$  would split into one orbit of size 2 and one of size 1. Choose  $y$  in the two-element orbit. By the Orbit-Stabiliser Theorem,

$$|G| = |G \cdot y| |G_y| = 2 |G_y|.$$

Hence  $|G_y| = |G|/2$ , but  $|G|$  is odd, so  $|G|/2 \notin \mathbb{Z}$  which is a contradiction.

Consequently an odd-order group cannot have a non-transitive, non-trivial action on a three-element set.