MATH 7210 Homework 3

Andrea Bourque

September 2021

1 Problem 1

Let G be a group with subgroups H, K.

(a) Show that the inverse of a bijective G-map is also a G-map.

Proof. Let $f : X \to Y$ be a bijective G-map. Let $y \in Y$ and let $x = f^{-1}(y)$, so $y = f(x)$. Then $f^{-1}(g \cdot y) = f^{-1}(g \cdot f(x)) = f^{-1}(f(g \cdot x)) = g \cdot x = g \cdot f^{-1}(y)$, showing that f^{-1} is a G-map. $\square$

(b) Show that if $f : X \to Y$ is a G-map, then for all $x \in X$, $\mathrm{Stab}(x) \subset \mathrm{Stab}(f(x))$.

Proof. Let $g \in \mathrm{Stab}(x)$. Then $f(x) = f(g \cdot x) = g \cdot f(x)$, showing that $g \in \mathrm{Stab}(f(x))$. $\square$

(c) Show that there exists a G-map $G/H \to G/K$ iff H is contained in a conjugate of K.

Proof. ($\to$) Let $f : G/H \to G/K$ be a G-map. Let $g \in G$ be such that $f(H) = gK$. For $h \in H$, $gK = f(H) = f(hH) = hf(H) = hgK$. Thus for some $k \in K$, $gk = hg$, so $h = gkg^{-1}$. Thus $H \subset gKg^{-1}$.

($\leftarrow$) Suppose $H \subset gKg^{-1}$. Define $f : G/H \to G/K$ by $f(aH) = agK$. This is well-defined since for any $h \in H$, there is some $k \in K$ such that $h = gkg^{-1}$, so $f(ahH) = ahgK = agkg^{-1}g = agkK = agK = f(aH)$. Furthermore, it is a G-map since $f(b \cdot aH) = f(baH) = bagK = b \cdot agK = b \cdot f(aH)$. $\square$

(d) Show that G/H and G/K are isomorphic G-sets iff K is a conjugate of H.

Proof. ($\to$) Since we have a bijective G-map $G/H \to G/K$, we have H is contained in a conjugate of K, or equivalently, K contains a conjugate of H. Since the inverse is also a G-map $G/K \to G/H$, we have K is contained in a conjugate of H. Therefore K contains a conjugate of H, and is also contained in a conjugate of H. This implies K is a conjugate of H.

($\leftarrow$) Suppose $K = gHg^{-1}$. Then as in the proof of (c), we have a G-map $f : G/K \to G/H$ defined by $f(aK) = agH$. Now, $H = g^{-1}Kg$, so there is a G-map $f' : G/H \to G/K$ defined by $f'(aH) = ag^{-1}K$. Now, $f(f'(aH)) =$

$f(ag^{-1}K) = ag^{-1}gH = aH$ and $f'(f(aK)) = f'(agH) = agg^{-1}K = aK$, so $f' = f^{-1}$, implying f is an isomorphism. $\square$

2 Problem 2

Let G be abelian with order $p^n m$, where p is prime and p, m are coprime. Let $P = \{a \in G \mid a^{p^k} = e \text{ for some } k \geq 0\}$. Prove the following:

(a) $P \leq G$.

Proof. Clearly $e \in P$ since $e^{p^0} = e$. Let $a, b \in P$ such that $a^{p^k} = e, b^{p^l} = e$. Since G is abelian, $(ab)^r = a^r b^r$ for any r. Thus $(ab)^{p^{k+l}} = a^{p^k p^l} b^{p^k p^l} = e$, so $ab \in P$. $(a^{-1})^{p^k} = (a^{p^k})^{-1} = e$, so $a^{-1} \in P$. Thus $P \leq G$. $\square$

(b) G/P has no elements of order p.

Proof. If xP is an element of order p, then $x^p \in P$. Then for some $k \geq 0$, $(x^p)^{p^k} = e$. But $(x^p)^{p^k} = x^{p^{k+1}}$, which shows $x \in P$, so that xP is the identity in G/P, which has order 1. $\square$

(c) $|P| = p^n$.

Proof. By Cauchy's theorem, if p divided $|G/P|$, then there would be an element of order p. Therefore, $|G/P| = |G|/|P|$ has no factor of p, implying that P has a factor of p^n, since $|G| = p^n m$ and m has no factor of p. If $|P|$ had a prime factor $q \neq p$, then there would be an element $a \in P$ of order q. But for some $k \geq 0$, $a^{p^k} = e$, which means $|a| = q$ divides p^k. The only prime dividing p^k is p, meaning that $q = p$. Therefore, $|P|$ has no prime factor other than p. Furthermore, since the highest power of p dividing $|G|$ is p^n, P cannot be larger than p^n. Thus $|P| = p^n$. $\square$

(d) P is the unique subgroup of order p^n.

Proof. Let P' be a subgroup of order p^n. Then the order of every element in P' divides p^n, meaning that every element in P' has an order p^k for $0 \leq k \leq n$. It follows that $P' \subset P$, since by definition, P consists of *all* elements with order p^k for some $k \geq 0$. But $|P'| = |P|$, so $P' = P$. $\square$

3 Problem 3

Let $G = GL_2(\mathbb{Z}/p\mathbb{Z})$, where p is prime. Consider the action of G on $(\mathbb{Z}/p\mathbb{Z})^2$.

(a) Show that G acts transitively on $X = (\mathbb{Z}/p\mathbb{Z})^2 - \{(0,0)\}$.

Proof. Let $(w,x),(y,z) \in X$. We consider cases.

Case 1: $w \neq 0, x = 0$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w \\ 0 \end{pmatrix} = \begin{pmatrix} aw \\ cw \end{pmatrix}$, so we let $a = w^{-1}y, c = w^{-1}z$. y, z are not both zero. If $y \neq 0$, let $b = 0, d = 1$, so that the determinant is $w^{-1}y \neq 0$. Otherwise, if $z \neq 0$, let $d = 0, b = 1$, so the determinant is $-w^{-1}z \neq 0$.

Case 2: $w = 0, x \neq 0$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ x \end{pmatrix} = \begin{pmatrix} bx \\ dx \end{pmatrix}$, so we let $b = x^{-1}y, d = x^{-1}z$. Again, y, z are not both zero. If $y \neq 0$, let $c = 1, a = 0$ so the determinant is $-x^{-1}y \neq 0$. Otherwise, if $z \neq 0$, let $a = 1, c = 0$, so the determinant is $x^{-1}z \neq 0$.

Case 3: $w \neq 0, x \neq 0$. We consider three subcases.

Subcase 1: $y \neq 0, z \neq 0$. We let $a = w^{-1}y, d = x^{-1}z, b = c = 0$. The determinant is $w^{-1}x^{-1}yz \neq 0$.

Subcase 2: $y = 0, z \neq 0$. We must have $aw + bx = 0$, so let $b = 1$ so that $a = -w^{-1}x$. Then let $d = 0$, so $c = w^{-1}z$ and the determinant is $-w^{-1}z \neq 0$.

Subcase 3: $y \neq 0, z = 0$. We must have $cw + dx = 0$, so let $d = 1$ so that $c = -w^{-1}x$. Then let $b = 0$, so $a = w^{-1}y$ and the determinant is $w^{-1}y \neq 0$. □

(b) Compute $\text{Stab}(1,0)$.

Proof. Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then $a = 1, c = 0$. The determinant of the matrix is then d, so in order for it to be invertible, we must have $d \neq 0$. Thus $\text{Stab}(1,0) = \{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}, d \neq 0\}$. □

(c) What is $|G|$?

Proof. Since G acts transitively, the orbit of $(1,0)$ is X. $|X| = p^2 - 1$, since $(\mathbb{Z}/p\mathbb{Z})^2$ has p^2 elements, since there are p choices for each entry and we subtract one for $(0,0)$. The stabilizer of $(1,0)$ has a size $p(p-1)$, since there are p choices for b and $p-1$ choices for d, since $d \neq 0$. Thus by the orbit-stabilizer theorem, we have $|G| = p(p-1)(p^2-1)$. □

4 Problem 3.3.3

If $H \lhd G$ of prime index p, then for all $K \leq G$, either $K \leq H$ or $G = HK$ and $|K : K \cap H| = p$.

Proof. Suppose K is not a subgroup of H. Since H is normal, $HK \leq G$. Furthermore, since there exists some element $x \in K$ which is not in H, HK also contains x since $x = ex$ is a product of an element of H and an element of K. But $H \subset HK$ since any $h \in H$ can be expressed as he, a product of an element of H and an element of K. Therefore, HK is a subgroup of G strictly containing H. Then $|G : HK|$ divides, and is less than, p, meaning $|G : HK| = 1$, meaning that $HK = G$. $\square$

5 Problem 4.1.9

Assume G acts transitively on the finite set A and let $H \triangleleft G$. Let $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_i$ in the sense that for each $g \in G$ and $i = 1, ..., r$, $g\mathcal{O}_i = \mathcal{O}_j$ for some j. Furthermore, show that G is transitive on the sets $\mathcal{O}_i$. Deduce that the $\mathcal{O}_i$ all have the same cardinality.

Proof. Let x_i be a representative for the orbit $\mathcal{O}_i$, so that any $x \in \mathcal{O}_i$ is equal to $h \cdot x_i$ for some $h \in H$. Then $g \cdot x = g \cdot (h \cdot x_i) = (gh) \cdot x_i = (h'g) \cdot x_i = h' \cdot (g \cdot x_i)$, where $gh = h'g$ for some $h' \in H$ follows from normality of H. Thus the action of g on an element of $\mathcal{O}_i$ is in the orbit of $g \cdot x_i$ under H, so G permutes the orbits.

Since G acts transitively on A, given an orbit $\mathcal{O}_i$ with representative x_i and any other orbit $\mathcal{O}_j$ with representative x_j, there is a $g \in G$ such that $g \cdot x_i = x_j$, so that g sends the orbit $\mathcal{O}_i$ to the orbit $\mathcal{O}_j$.

Since for each i there is g_i such that $g_i\mathcal{O}_1 = \mathcal{O}_i$, and since $|g_i\mathcal{O}_1| = |\mathcal{O}_1|$, it follows that all the orbits have the same cardinality. □

(b) Prove that if $a \in \mathcal{O}_1$, then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$.

Proof. $H \cap G_a$ consists of those $h \in H$ which stabilize a. Thus, by the orbit stabilizer theorem for the action of H on A, $|\mathcal{O}_1| = |H : H \cap G_a|$.

Now we consider the transitive action of G on the orbits. By the orbit-stabilizer theorem, r is equal to the index in G of the stabilizer of some orbit, say $\mathcal{O}_1$. Let $g\mathcal{O}_1 = \mathcal{O}_1$. Then $g \cdot a = h \cdot a$ for $h \in H$. Thus if g fixes $\mathcal{O}_1$, $h^{-1}g \in G_a$ for some $h \in H$. Thus $g \in HG_a$. Conversely, if $g \in HG_a$, say $g = hk$ for $h \in H, k \in G_a$, then $g\mathcal{O}_1$ is the orbit of $g \cdot a = (hk) \cdot a = h \cdot a$, which is in the orbit of a. Thus HG_a is exactly the subgroup which fixes $\mathcal{O}_1$, showing that $r = |G : HG_a|$. □