Silvain Rideau silvain.rideau@berkeley.edu
1091 Evans www.normalesup.org/~srideau/en/teaching

Solutions to the midterm

October 21st

Problem 1 :
These questions were covered in class.

1. Let G be a group acting on a set X and let $x \in X$. Define $\mathrm{Stab}_G(x)$ and show that it is a subgroup of G.

   Solution: We have $\mathrm{Stab}_G(x) = \{g \in G : g \star x = x\}$.

   Since $1 \star x = x$ by definition of a group action, we have $1 \in \mathrm{Stab}_G(x)$. Also, for all g, $h \in \mathrm{Stab}_G(x)$, $(g \cdot h) \star x = g \star (h \star x) = g \star x = x$ so $g \cdot h \in \mathrm{Stab}_G(x)$. Finally, for all $g \in \mathrm{Stab}_G(x)$, $x = 1 \star x = (g^{-1} \cdot g) \star x = g^{-1} \star g \star x = g^{-1} \star x$ so $g^{-1} \in \mathrm{Stab}_G(x)$. So $\mathrm{Stab}_G(x) \leqslant G$.

2. Show that the kernel of a group homomorphism is normal.

   Solution: Let $f : G \to H$ be a group homomorphism. We have to show that, for all $g \in G$, $g \ker f g^{-1} \subseteq \ker f$. For all $h \in \ker f$, we have $f(g \cdot h \cdot g^{-1}) = f(g) \cdot f(h) \cdot f(g)^{-1} = f(g) \cdot 1 \cdot f(g)^{-1} = 1$. It follows that $g \cdot h \cdot g^{-1} \in \ker f$ and hence $g \ker f g^{-1} \subseteq \ker f$. So $\ker f$ is normal.

3. State the first isomorphism theorem.

   Solution: Let $f : G \to H$ be a group homomorphism. Then $\ker f$ is a normal subgroup of G and $G/\ker f \cong f(G)$.

Problem 2 :
Let G be a group. We define $X := \{(x_0, x_1 \ldots, x_{p-1}) : \prod_{i=0}^{p-1} x_i = 1\}$.

1. Show that $|X| = |G|^{p-1}$.

   Solution: The map $f : X \to G^{p-1}$ defined by $(x_0, \ldots, x_{p-1}) \mapsto (x_1, \ldots, x_{p-1}$ is a bijection. Indeed, if $x_0, \ldots, x_{p-1}) \in X$, then $\prod_{i=0}^{p-1} x_i = 1$ so $x_0 = (\prod_{i=1}^{p-1} x_i)^{-1}$ and hence the first element is completely dertemined by the other $p-1$ elements of the tuple and f is injective. Moreover for all $(x_1, \ldots, x_{p-1}) \in G^{p-1}$, setting $x_0 = (\prod_{i=!}^{p-1} x_i)^{-1}$, we get an element of X, so f is surjective.

   Since f is a bijection, we have $|X| = |G^{p-1}| = |G|^{p-1}$.

   This is the formal way of saying that we can choose "freely" $p-1$ elements of the tuple and the last one is given by the inverse.

2. Show that if $(x_0, \ldots, x_{p-1}) \in X$, then for all $0 < n < p$, we have:

   $$(x_n, x_{n+1} \ldots, x_{p-1}, x_0, \ldots, x_{n-1}) \in X.$$

   Solution: Since $\prod_{i=0}^{p-1} x_i = (\prod_{i=0}^{n-1} x_i) \cdot (\prod_{i=n}^{p-1} x_i) = 1$, we have that $\prod_{i=0}^{n-1} x_i = (\prod_{i=n}^{p-1} x_i)^{-1}$ and hence $x_n \cdot \cdots \cdot x_{p-1} \cdots x_0 \cdot \cdots \cdot x_{n-1} = (\prod_{i=n}^{p-1} x_i) \cdot (\prod_{i=n}^{p-1} x_i)^{-1} = 1$ and we do have $(x_n, x_{n+1} \ldots, x_{p-1}, x_0, \ldots, x_{n-1}) \in X$.

3. Let $\sigma \in S_p$ be the cycle $(0\,1\ldots p-1)$. Show that

$$n \star (x_0, \ldots, x_{p-1}) := (x_{\sigma^n(0)}, \ldots, x_{\sigma^n(p-1)})$$

defines an action of $\mathbb{Z}$ on X.

Solution: First of all, let r be the remainder of the division of n by p, we have $n \star (x_0, \ldots, x_{p-1}) = x_r, \ldots, x_{p-1}, x_0, , x_{r-1}$ and hence, by the previous question $n \star (x_0, \ldots, x_{p-1}) \in X$. Moreover, $0 \star (x_0, \ldots, x_{p-1}) = (x_{\sigma^0(0)}, \ldots, x_{\sigma^0(p-1)}) = (x_0, \ldots, x_{p-1})$ and, for all n, $m \in \mathbb{Z}$, $n \star (m \star (x_0, \ldots, x_{p-1})) = n \star (x_{\sigma^m(0)}, \ldots, x_{\sigma^m(p-1)}) = (x_{\sigma^n(\sigma^m(0))}, \ldots, x_{\sigma^n(\sigma^m(p-1))}) = (x_{\sigma^{n+m}(0)}, \ldots, x_{\sigma^{n+m}(p-1)}) = (n+m) \star (x_0, \ldots, x_{p-1})$. So $\star$ defines an action of $\mathbb{Z}$ on X.

4. Show that for all $x \in X$, $p\mathbb{Z} \subseteq \mathrm{Stab}_{\mathbb{Z}}(x)$.

Solution: Since σ is a p-cycle, for all $n \in \mathbb{Z}$, $\sigma^{np} = (\sigma^p)^n$ is the identity map. It follows that $(np) \star (x_0, \ldots, x_{p-1}) = (x_{\sigma^{np}(0)}, \ldots, x_{\sigma^{np}(p-1)}) = (x_0, \ldots, x_{p-1})$ and $np \in \mathrm{Stab}_{\mathbb{Z}}(x)$. Since n was any elements of $\mathbb{Z}$, we have just proved that $p\mathbb{Z} \subseteq \mathrm{Stab}_{\mathbb{Z}}(x)$.

5. Show that for all $x \in X$, the orbit of x has size 1 or p.

Solution: We know that for all $x \in X$, $|\mathbb{Z} \star x| = [\mathbb{Z} : \mathrm{Stab}_{\mathbb{Z}}(x)]$. Since $\mathrm{Stab}_{\mathbb{Z}}(x)$ is a subgroup of $\mathbb{Z}$ which is cyclic it must be of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Since it contains $p\mathbb{Z}$ and p is prime, by the classification of subgroups in infinite cyclic groups, we must have $n|p$ and hence $\mathrm{Stab}_{\mathbb{Z}}(x)$ is either $\mathbb{Z}$ or $p\mathbb{Z}$ and its index in $\mathbb{Z}$ is either 1 or p.

6. Show that the orbit of x has size 1 if and only if $x = (x_0, x_0, \ldots, x_0)$.

Solution: Let us first assume that $x = (x_0, \ldots, x_p)$ where $x_i = x_0$ for all i. Then, for all $n \in \mathbb{Z}$, $n \star x = (x_{\sigma^n(0)}, \ldots, x_{\sigma^n(p-1)}) = (x_0, \ldots, x_0) = x$ and the orbit of x is a singleton.

Conversely, assume that the orbit of x is a singleton, then $1 \star x = (x_1, \ldots, x_{p-1}, x_0) = x = (x_0, \ldots, x_{p-2}, x_{p-1})$. It follows that the coordinates of those two tuples must be equal and hence $x_i = x_{i+1}$ for all i. By induction, $x_i = x_0$ for all i

7. Assume that p divides $|G|$. Show that p divides the number of orbits of size 1. Deduce (without using Cauchy's theorem) that there is an element of order p in G.

Solution: We have that $|X| = \sum_{i=0}^{k-1} |\mathbb{Z} \star x_i|$ where the x_i are representatives of the orbits. Reordering them, we may assume that for all $i < l$, $|\mathbb{Z} \star x_i| = 1$ and that for all $igeql$, $|\mathbb{Z} \star x_i| > 1$. In that last case, it must be equal to p. We have $0 \equiv |G|^{p-1} \equiv |X| \equiv l + p(k-l) \equiv l \mod p$. So l is also divisible by p. Moreover, $(1, \ldots, 1) \in X$ has an orbit of size 1 and thus $l > 0$. It follows that $l \geqslant p$ and therefore, there is an $x \in G \setminus \{1\}$ such that $(x, \ldots, x) \in X$, i.e. $x^p = 1$. Since $x \neq 0$, $|x| = p$.