Silvain Rideau
1091 Evans

silvain.rideau@berkeley.edu
www.normalesup.org/~srideau/en/teaching

Solutions to homework 3

Due September 18th

Problem 1 :
Let G be a finite group and $n = |G|$.

1. For any $a \in G$, let $f_a(x) = a \cdot x$. Show that $a \mapsto f_a$ is an injective group homomorphism from G into S_G.

   Solution: We have first to check that $f_a : G \to G$ is a bijection. Because G is finite, it suffices to check it is an injection (but this map will also be a bijection when G is not finite). Assume $a \cdot x = a \cdot y$, then $x = y$ and hence f_a is injective.

   So $\varphi : a \mapsto f_a$ is a map from G into S_G. We have to check that it is an injective homomorphism. Let a, $b \in G$ and $x \in G$, then $f_{ab}(x) = abx = f_a \circ f_b(x)$. So the maps f_{ab} and $f_a \circ f_b(x)$ are equal and φ is a homomorphism.

   Let us now show it is injective. Assume that $f_a = \mathrm{id}$, then $f_a(1) = a \cdot 1 = a = 1$, so $\ker(\varphi) = \{1\}$ and φ is injective.

2. Show that every finite group is isomorphic to a subgroup of $S_{\mathbb{Z}_{>0}}$.

   Solution: We have just shown that G is isomorphic to a subgroup of S_G which is itself isomorphic to $S_{|G|}$. To conclude, is suffices to show that S_n is isomorphic to a subgroup of $S_{\mathbb{N}}$ (and take $n = |G|$). Let $\theta : S_n \to S_{\mathbb{N}}$ be the map that send $\sigma \in S_n$ to the bijection of $S_{\mathbb{N}}$ that fixes every $x \geqslant n$ and acts as σ on $\{0, \ldots, n-1\}$. Let σ and $\tau \in S_n$ and $x \in \mathbb{N}$. If $x \geqslant n$, $\theta(\sigma \circ \tau)(x) = x = \theta(\sigma) \circ \theta(\tau)(x)$ and if $x < n$, $\theta(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \theta(\sigma) \circ \theta(\tau)(x)$, so θ is an homomorphism. The kernel of θ is easily seen to be $\{\mathrm{id}\}$ and hence θ is a monomorphism.

Problem 2 :
Let G be a finite group and $\sigma \in \mathrm{Aut}(G)$. Assume that for all $x \in G$, $\sigma(x) = x$ implies $x = 1$ and that $\sigma^2 = 1$ (in this equation, the product and identity are considered in the group $\mathrm{Aut}(G)$).

1. Show that the map $f : G \to G$ defined by $f(x) = x^{-1}\sigma(x)$ is a bijection.

   Solution: Let us first show that f is injective. If x, $y \in G$ are such that $x^{-1}\sigma(x) = f(x) = f(y) = y^{-1}\sigma(y)$, then $yx^{-1} = \sigma(y)\sigma(x)^{-1} = \sigma(yx^{-1})$. By hypothesis, it follows that $yx^{-1} = 1$, i.e. $x = y$. Moreover, since G is finite, any injection of G into itself is a surjection, so f is a bijection.

2. Show that for all $x \in G$, $\sigma(x) = x^{-1}$.

   Solution: Pick $y \in G$. By the previous question, $y = f(x) = x^{-1}\sigma(x)$ for some $x \in G$. So $\sigma(y) = \sigma(x^{-1}\sigma(x)) = \sigma(x)^{-1}\sigma^2(x) = \sigma(x)^{-1}x = (x^{-1}\sigma(x))^{-1} = y^{-1}$.

3. Show that G is Abelian.

   Solution: Since σ is a group automorphism and $\sigma(x) = x^{-1}$, for all x, $y \in G$, we have $xy = \sigma(x^{-1})\sigma(y^{-1}) = \sigma(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = yx$.

Problem 3 :
If G is an Abelian group, let $\mathrm{tor}(G) := \{x \in G : |x| < \infty\}$. It is called the torsion group of G. For all $n \in \mathbb{Z}_{>0}$, let $Z_n := \{e^{\frac{2ik\pi}{n}} : k \in \mathbb{Z}\} \subseteq \mathbb{C}$. Let $Z := \bigcup_n Z_n$.

1. Show that $\mathrm{tor}(G) \leqslant G$.

   Solution: Pick any $a \in \mathrm{tor}(G)$. Then $|a^{-1}| = |a| = n < \infty$ so $a \in \mathrm{tor}(G)$. Let us now also pick $c \in \mathrm{tor}(G)$. Let $m := |c|$, then, because G is Abelian, $(ac)^{mn} = a^{mn}c^{mn} = 1$, so $|ac| < \infty$.

2. Show that $\mathrm{tor}(\mathbb{C}^\star) = Z$.

   Solution: Firstly, $(e^{\frac{2ik\pi}{n}})^n = (e^{2i\pi})^k = 1$, so $Z \subseteq \mathrm{tor}(\mathbb{C}^\star)$. Conversely, let $\alpha = re^{2i\theta\pi} \in \mathbb{C}$, where $r \in \mathbb{R}_{>0}$ and $\alpha \in \mathbb{R}$, be such that $\alpha^n = 1$ for some n. Then $r^n = 1$ so $r = 1$ and $n\theta = k \in \mathbb{Z}$ so $\theta = \frac{k}{n}$. It follows that $\alpha = e^{\frac{2ik\pi}{n}} \in Z$.

3. Pick some k dividing n. Show that the only subgroup of Z_n of order k is Z_k.

   Solution: Note that $Z_n = \{(e^{\frac{2i\pi}{n}})^k : k \in \mathbb{Z}\} = \langle e^{\frac{2i\pi}{n}} \rangle$ is cyclic. Moreover $(e^{\frac{2i\pi}{n}})^k = 1$ if and only if $n|k$ so $|e^{\frac{2i\pi}{n}}| = n = |Z_n|$. By the results proved in class about cyclic groups, there is a unique subgroup of order $k|n$ in Z_n. This group is $\langle (e^{\frac{2i\pi}{n}})^{\frac{n}{k}} \rangle = \langle (e^{\frac{2i\pi}{k}}) \rangle = Z_k$.

   But since the problem was asked before we knew what cyclic groups were, let us also prove it by hand. Let us first prove that if $k|n$, then $Z_k \leqslant Z_n$. Indeed, if $n = kl$, then for all $m \in \mathbb{Z}$, $e^{\frac{2im\pi}{k}} = e^{\frac{2iml\pi}{n}} \in Z_n$. Now, let $H \leqslant Z_n$ have order k. Assume $x := e^{\frac{2il\pi}{n}} \in H$ and let $d = \gcd(l, n)$. There exists $u, v, n_0 \in \mathbb{Z}$ such that $ul + vn = d$ and $n = dn_0$. Then $x^u = e^{\frac{2iul\pi}{n}} = e^{\frac{2i(d-vn)\pi}{n}} = e^{\frac{2id\pi}{n}} \cdot e^{2iv\pi} = e^{\frac{2i\pi}{n_0}} \in H$.

   Let $l_0 \in \mathbb{Z}_{>0}$ be minimal such that $e^{\frac{2il_0\pi}{n}} \in H$ and l_0 divides n—this minimum exists because $e^{\frac{2in\pi}{n}} = 1 \in H$. Then for all $x := e^{\frac{2il\pi}{n}} \in H$, if $l = l_0q + r$ with $q, r \in \mathbb{Z}$ and $0 \leqslant r < l_0$, then $x \cdot (e^{\frac{2il_0\pi}{n}})^{-q} = e^{\frac{2ir\pi}{n}} \in H$. By the above computation, if $r \neq 0$, and $d = \gcd(r, n)$, $e^{\frac{2id\pi}{n}} \in H$, but $d \leqslant r < l_0$, a contradiction. It follows that $r = 0$ and $H = \{(e^{\frac{2il_0\pi}{n}})^q : q \in \mathbb{Z}\} = Z_{\frac{n}{l_0}}$. Since $k = |H| = |Z_{\frac{n}{l_0}}| = \frac{n}{l_0}$, we are done.

4. Show that $Z_n \leqslant Z_m$ if and only if $n|m$.

   Solution: The statement that if $n|m$ then $Z_n \leqslant Z_m$ is proved in the previous question. Let us prove the converse. Assume $Z_n \leqslant Z_m$, then $e^{\frac{2i\pi}{n}} \in Z_m$ so there exists $k \in \mathbb{Z}$ such that $e^{\frac{2i\pi}{n}} = e^{\frac{2ik\pi}{m}}$. It follows that $e^{2i\pi(\frac{1}{n} - \frac{k}{m})} = 1$ and hence $\frac{1}{n} - \frac{k}{m} = l \in \mathbb{Z}$. Mulitplying by nm we obtain that $m = n(k + lm)$, i.e. $n|m$.

   Since we know that $|Z_n| = n$, we can also conclude by Lagrange (when we'll know Lagrange).

5. Show that there does not exists $a_1, \ldots, a_k \in Z$ such that $Z = \langle a_1, \ldots, a_k \rangle$

   Solution: Let us prove, first, that $\langle Z_n \cup Z_m \rangle = Z_{\mathrm{lcm}(m,n)}$. By Question 4, Z_n, $Z_m \leqslant Z_{\mathrm{lcm}(m,n)}$ so $\langle Z_n \cup Z_m \rangle \leqslant Z_{\mathrm{lcm}(m,n)}$. Let $d = \gcd(m, n)$. There exists u, $v \in \mathbb{Z}$ such that $un + vm = d$. Then $(e^{\frac{2i\pi}{n}})^v (e^{\frac{2i\pi}{m}})^u = e^{\frac{2i(vm+un)\pi}{mn}} = e^{\frac{2id\pi}{nm}} = e^{\frac{2i\pi}{\mathrm{lcm}(m,n)}}$. It follows that $Z_{\mathrm{lcm}(m,n)} = \langle e^{\frac{2i\pi}{\mathrm{lcm}(m,n)}} \rangle \leqslant \langle Z_n \cup Z_m \rangle$.

   Let us now prove by induction on k that $\langle a_1, \ldots, a_k \rangle = Z_n$ for some $n \in \mathbb{Z}_{>0}$. If $k = 0$, let $a_1 = e^{\frac{2il\pi}{n}}$ where $\gcd(l, n) = 1$. There exists u, $v \in \mathbb{Z}$ such that $ul + vn = 1$.

We have $a_1^u = e^{\frac{2iul\pi}{n}} = e^{\frac{2i(1-vn)\pi}{n}} = e^{\frac{2i\pi}{n}}$. So $e^{\frac{2i\pi}{n}} \in \langle a_1 \rangle$. Since $a_1 = (e^{\frac{2i\pi}{n}})^l$, we also have $a_1 \in \langle e^{\frac{2i\pi}{n}} \rangle = Z_n$ so $\langle a_i \rangle = Z_n$.

Let us now this holds for k and pick $a_1, \dots, a_{k+1} \in Z$. By induction, we find $n \in \mathbb{Z}_{>0}$ such that $\langle a_1, \dots, a_k \rangle = Z_n$. By the case $k = 1$ case we also find $m \in \mathbb{Z}$ such that $\langle a_{k+1} \rangle = Z_m$. It is easy to check that $\langle a_1, \dots, a_{k+1} \rangle = \langle Z_n \cup Z_m \rangle = Z_{\mathrm{lcm}(m,n)}$. Indeed, any group containing $\{a_i : 0 < i \leqslant k+1\}$ contains $\{a_i : 0 < i \leqslant k\}$ so it contains $\langle a_1, \dots, a_k \rangle = Z_n$. It also contains $\langle a_{k+1} \rangle = Z_m$ so it contains $\langle Z_n \cup Z_m \rangle$. Conversely, any group containing $Z_n \cup Z_m$ contains $\{a_i : 0 < i \leqslant k+1\}$ and hence $\langle a_1, \dots, a_{k+1} \rangle$.

So we have $\langle a_1, \dots, a_{k+1} \rangle = Z_m$ for some m. To conclude it suffices to show that $Z_m \subset Z$. But $e^{\frac{2i\pi}{m+1}} \in Z \setminus Z_m$. Otherwise we would have $e^{\frac{2i\pi}{m+1}} = e^{\frac{2ik\pi}{m}}$ for some $k \in \mathbb{Z}$. That would imply that $\frac{1}{m+1} - \frac{k}{m} = l \in \mathbb{Z}$ and hence $m = (lm+k)(m+1)$. It would follow that $m+1 | m$, a obvious contradiction since $m > 0$.

There is in fact a faster way of solving that question. The group Z is Abelian so $\langle a_1, \dots, a_k \rangle = \{\prod_i a_i^{k_i} : k_i \in \mathbb{Z}\}$. Since every a_i has finite order, we have, in fact, $\langle a_1, \dots, a_k \rangle = \{\prod_i a_i^{k_i} : 0 \leqslant k_i < |a_i|\}$ and so $|\langle a_1, \dots, a_k \rangle| \leqslant \prod_i |a_i| < \infty$. But Z is infinite (indeed, by an argument similar to the one above, all the $e^{\frac{2i\pi}{p}}$, for p prime, are distinct). So we cannot have $Z = \langle a_1, \dots, a_k \rangle$.