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

Solutions to the midterm

February 13th

Problem 1 :
The following questions are about material covered in class. When asked to prove something you are only allowed to use results that we proved before that particular result.

1. Define the center of a group and prove it is a subgroup.

   Solution: The center of a group G is $\mathrm{Z}(G) \coloneqq \{g \in G : \forall h \in G\ g \cdot h = h \cdot g\}$. Since, for all $h \in G$, $h \cdot 1 = 1 \cdot h$, we have $1 \in \mathrm{Z}(G)$. For all $g, h \in \mathrm{Z}(G)$ and all $x \in G$, we have $g \cdot h \cdot x = g \cdot x \cdot h = x \cdot g \cdot h$ so $g \cdot h \in \mathrm{Z}(G)$. Moreover, $x \cdot g^{-1} = g^{-}1 \cdot g \cdot x \cdot g^{-1} = g^{-1} \cdot x \cdot g \cdot g^{-1} = g^{-1} \cdot x$, so $g^{-1} \in \mathrm{Z}(G)$ and $\mathrm{Z}(G)$ is a subgroup of G.

2. Prove that every infinite cyclic group is isomorphic to $\mathbb{Z}$.

   Solution: Let $G = \langle x \rangle$ be infinite. Then $|x|$ is also infinite, otherwise $|\langle x \rangle| = |x|$ would be finite. Let $f : \mathbb{Z} \to G$ be defined by $i \mapsto x^i$. We have that $f(i+j) = x^{i+j} = x^i \cdot x^j = f(i) \cdot f(j)$, so f is a group homomorphism. Since $G = \langle x \rangle$, f is surjective and, for all $i \leqslant j \in \mathbb{Z}$, if $f(i) = x^i = x^j = f(j)$, then $x^{j-i} = 1$ where $j - i \in \mathbb{Z}_{\geqslant 0}$. By definition of $|x| = \infty$, $j - i = 0$, so f is injective. We have proved that f is a group isomorphism between G and $\mathbb{Z}$.

Problem 2 :

1. Compute the disjoint cycle decomposition and the order of the product $(0,1,2) \cdot (2,3) \cdot (0,1,2,3)$.

   Solution: Let $\sigma_1 = (0,1,2)$, $\sigma_2 = (2,3)$ and $\sigma_1 = (0,1,2,3)$. We have $\sigma_1 \cdot \sigma_2 \cdot \sigma_3(0) = \sigma_2 \cdot \sigma_2(1) = \sigma_1(1) = 2$, $\sigma_1 \cdot \sigma_2 \cdot \sigma_3(2) = \sigma_2 \cdot \sigma_2(3) = \sigma_1(2) = 0$, $\sigma_1 \cdot \sigma_2 \cdot \sigma_3(1) = \sigma_2 \cdot \sigma_2(2) = \sigma_1(3) = 3$ and $\sigma_1 \cdot \sigma_2 \cdot \sigma_3(3) = \sigma_2 \cdot \sigma_2(0) = \sigma_1(0) = 1$. So $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 = (0,2) \cdot (1.3)$.

   It is a product of two disjoint 2-cycles, so it is order $2 = \mathrm{lcm}(2,2)$.

2. Let $\tau = (0,1) \in S_n$, for $n \geqslant 2$. Show that $\sigma \in \mathrm{C}_{S_n}(\tau)$ if and only if $\sigma(\{0,1\}) = \{0,1\}$.

   Solution: Let us first assume that $\sigma(\{0,1\}) = \{0,1\}$. If $x \notin \{0,1\}$, then $\sigma(x) \notin \{0,1\}$ by injectivity and hence, $\tau \cdot \sigma(x) = \tau(\sigma(x)) = \sigma(x) = \sigma(\tau(x)) = \sigma \cdot \tau(x)$. If $x \in \{0,1\}$, then $\sigma(0) = 0$, in which case $\sigma(1) = 1$ or $\sigma(0) = 1$, in which case $\sigma(1) = 0$. In both cases, $\sigma(1-x) = 1 - \sigma(x)$. Then, $\tau \cdot \sigma(x) = 1 - \sigma(x)$ and $\sigma \cdot \tau(x) = \sigma(1-x) = 1 - \sigma(x)$. So $\sigma \cdot \tau = \tau \cdot \sigma$, i.e. $\sigma \in \mathrm{C}_{S_n}(\tau)$.

   Conversely, assume that $\sigma \in \mathrm{C}_{S_n}(\tau)$. If $x \notin \{0,1\}$ but $\sigma(x) \in \{0,1\}$, $\sigma \cdot \tau(x) = \sigma(x) = \tau(\sigma(x)) = 1 - \sigma(x)$, a contradiction. It follows that if $x \notin \{0,1\}$, then $\sigma(x) \notin \{0,1\}$. The function $\sigma|_{\{2,\dots n-1\}} : \{2,\dots n-1\} \to \{2,\dots n-1\}$ is an injection which is therefore surjective. If $\sigma(0) \in \{2,\dots,n-1\}$, then $\sigma(0) = \sigma(x)$ for some $x \in \{2,\dots n-1\}$, a contradiction. So $\sigma(0) \in \{0,1\}$. Similarly, $\sigma(1) \in \{0,1\}$.

   The converse can also been proven using the following formula that we have not proved in class yet but that you may have used for homework 2: if $\sigma \in \mathrm{C}_{S_n}(\tau)$, $(0,1) = \sigma \cdot (0,1) \cdot \sigma = (\sigma(0), \sigma(1))$, so $\sigma(\{0,1\}) = \{0,1\}$.

Problem 3 :
Let G be a group and p be some prime number.

1. Let $a, b \in G$ be such that $|a| = |b| = p$. Show that either $\langle a \rangle = \langle b \rangle$ or $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   Solution: Since the intersection of subgroups is a subgroup, $\langle a \rangle \cap \langle b \rangle$ is a subgroup of G and therefore of $\langle b \rangle$. Since p is prime, by Lagrange, $|\langle a \rangle \cap \langle b \rangle|$ is either 1 or p. If it is 1, then $\langle a \rangle \cap \langle b \rangle = \{1\}$. If it is p, then $\langle a \rangle \cap \langle b \rangle = \langle b \rangle$ and hence $\langle b \rangle \subseteq \langle a \rangle$. Since both have order p, $\langle a \rangle = \langle b \rangle$.

2. Let a and b be as above. Assume that $a \notin \langle b \rangle$, show that $\{a^i b^j : i, j \in \mathbb{Z}\}$ has at least p^2 elements.

   Solution: Since $a \notin \langle b \rangle$, we cannot have $\langle a \rangle = \langle b \rangle$, so, by the previous question, $\langle a \rangle \cap \langle b \rangle = \{1\}$. Let us now pick $0 \leqslant i_1 \leqslant i_2 < p$ and $0 \leqslant j_1 \leqslant j_2 < p$, if $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$, then $a^{i_1 - i_2} = b^{j_2 - j_1} \in \langle a \rangle \cap \langle b \rangle = \{1\}$, so $i_1 - i_2 \equiv j_2 - j_1 \equiv 0 \mod p$. Since $-p < i_1 - i_2 \leqslant 0$ and $0 \leqslant j_2 - j_1 < p$, it follows that $i_1 = i_2$ and $j_1 = j_2$. So the elements $a^i b^j$ for $0 \leqslant i, j < p$ are all distinct and there are p^2 of them.

3. Assume that G is Abelian, $|G| = p^2$ and that every element in $G \setminus \{1\}$ is order p. Show that $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

   Solution: Let $a \in G \setminus \{1\}$ be any element. Since $|G| = p^2$ and $|a| = p$, we have $\langle a \rangle < G$. Let $b \in G \setminus \rangle a \langle$ be any element. By the previous question, $\{a^i b^j : i, j \in \mathbb{Z}\} \subseteq G$ has at least p^2 elements so it is equal to G.

   Let us define $f : G \to (\mathbb{Z}/p\mathbb{Z})^2$ by $f(a^i b^j) = (\overline{i}, \overline{j})$. Let us check that f is well defined. If $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$, then, as see above, we must have $i_1 \equiv i_2 \mod p$ and $j_1 \equiv j_2 \mod p$, so f is well defined. Let us check it is an homomorphism $f(a^{i_1} b^{j_1} a^{i_2} b^{j_2}) = f(a^{i_1 + i_2} b^{j_1 + j_2}) = (\overline{i_1 + i_2}, \overline{j_1 + j_2}) = (\overline{i_1}, \overline{j_1}) + (\overline{i_2}, \overline{j_2}) = f(a^{i_1} b^{j_1}) + f(a^{i_2} b^{j_2})$ where the last two + denote the operation on $(\mathbb{Z}/p\mathbb{Z})^2$, i.e. coordinatewise addition. Finally f is injective, indeed if $i_1 \equiv i_2 \mod p$ and $j_1 \equiv j_2 \mod p$, $a^{i_1} = a^{i_2}$ and $b^{j_1} = b^{j_2}$ so $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$. Since $|G| = p^2 = |(\mathbb{Z}/p\mathbb{Z})^2|$, f is an isomorphism.