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

Solutions to the midterm

September 21st

Problem 1 :

1. Show that a group homomrphism f is injective if and only if $\ker(f) = \{1\}$.

   Solution: Let us first show that if $f : G \to H$ is injective then $\ker(f) = \{1\}$. Recall that $\ker(f) = f^{-1}(1) = \{g \in G : f(g) = 1\}$. Since f is a homomorphism, $f(1) = 1$. Now let us assume that $f(g) = 1 = f(1)$. Since f is injective, $g = 1$ and therefore $\ker(f) = \{g \in G : f(g) = 1\} = \{1\}$.

   Conversely, let us assume that $\ker(f) = \{1\}$. Pick any $g, h \in G$ such that $f(g) = g(h)$. It follows that $f(g \cdot h^{-1}) = f(g) \cdot f(h)^{-1} = 1$ and hence that $g \cdot h^{-1} \in \ker(f) = \{1\}$. Since $g \cdot h^{-1} = 1$, we must have $g = h$.

2. Define what a k-cycle in S_n is.

   Solution: A permutation $\sigma \in S_n$ is a k-cycle if there exists $a_1, \ldots, a_k \in \{1, \ldots, n\}$ distinct such that for all $i \in \{1, \ldots, k-1\}$, $\sigma(a_i) = \sigma(ai+1)$, $\sigma(a_k) = \sigma(a1)$ and for all $x \in \{1, \ldots, n\} \smallsetminus \{a_1, \ldots, a_k\}$, $\sigma(x) = x$.

   Equivalently, we can say that there are distinct elements $a_{\bar{i}}$ for all $\bar{i} \in \mathbb{Z}/k\mathbb{Z}$ such that $\sigma(a_{\bar{i}}) = \sigma(a_{\bar{i}+\bar{1}})$ and σ fixes all the other elements of $\{1, \ldots, n\}$.

3. Show that two disjoint cycles commute.

   Solution: Let $\sigma, \tau \in S_n$ be two disjoint cycles. We have $\sigma = (a_{\bar{1}} \ldots a_{\bar{k}})$ and $\tau = (b_{\bar{1}} \ldots b_{\bar{l}})$ where $a_{\bar{i}}, b_{\bar{j}} \in \{1, \ldots, n\}$ are all distinct. For all $\bar{i} \in \mathbb{Z}/k\mathbb{Z}$, we have $\tau(\sigma(a_{\bar{i}})) = \tau(a_{\bar{i}+\bar{1}}) = a_{\bar{i}+\bar{1}}$ and $\sigma(\tau(a_{\bar{i}})) = \sigma(a_{\bar{i}}) = a_{\bar{i}+\bar{1}}$. Similarly, for all $\bar{j} \in \mathbb{Z}/l\mathbb{Z}$, we have $\tau(\sigma(b_{\bar{j}})) = \tau(b_{\bar{j}}) = b_{\bar{j}+\bar{1}} = \sigma(b_{\bar{j}+\bar{1}}) = \sigma(\tau(b_{\bar{j}}))$. Finally, if x is neither $a_{\bar{i}}$ or $b_{\bar{j}}$, then $\tau(\sigma(x)) = \tau(x) = x = \sigma(x) = sigma(\tau(x))$.

   It follows that $\tau \circ \sigma = \sigma \circ \tau$.

Problem 2 :
Let G be a group whose only subgroups are $\{1\}$ and G. Show that G is isomorphic to $\{1\}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Solution: If $G = \{1\}$, then it is isomorphic to the trivial group. If not, let $x \in G$ not be the identity. We have $\{1\} < \langle x \rangle \leqslant G$. By hypothesis on G it follows that G is cyclic.
If $card x = \infty$, then $\{1\} < \langle x^2 \rangle < G$, contradicting our hypothesis on G. So $|x| = n < \infty$ and $G \simeq \mathbb{Z}/n\mathbb{Z}$. There remains to show that n is prime. Since $G = \langle x \rangle$, for all $k|n$, there is a subgroup $H \leqslant G$ of order k. By hypothesis on G, we must have $H = \{1\}$ or $H = G$, i.e. $k = 1$ or $k = n$. So the only divisors of n are 1 and itself (and $n \neq 1$ since $\{1\} < G$) and n is prime.

Problem 3 :

1. Let $A = \{1, s, r^2, sr^2\} \subset D_8$, compute $C_{D_8}(A)$ and $N_{D_8}(A)$.

   Solution: We have $s1s^{-1} = 1$, $sr^2s^{-1} = r^{-2} = r^2$, $sss^{-1} = s$ and $ssr^2s^{-1} = sr^{-2} = sr^2$ so $s \in C_{D_8}(A)$. Similarly, $r^2 1 r^{-2} = 1$, $r^2r^2r^{-2} = r^2$, $r^2sr^{-2} = r^4s = s$ and $r^2sr^2r^{-2} = sr^{-2} = sr^2$ so $r^2 \in C_{D_8}(A)$. Since $C_{D_8}(A) \leqslant D_8$, all the products of s and r^2 are also in $C_{D_8}(A)$ and thus $A \subseteq C_{D_8}$.

   Now $rsr^{-1} = sr^2 \neq s$ so $r \notin A$, since $C_{D_8}(A) \leqslant D_8$, we cannot have $r^3 = rr^2$, sr and $sr^3 = sr^2r$ in $C_{D_8}(A)$ either. So $C_{D_8}(A) = A$.

   We have $s \in C_{D_8}(A) \subseteq N_{D_8}(A)$. Moreover, $r1r^{-1} = 1 \in A$, $rsr^{-1} = sr^2 \in A$, $rr^2r^{-1} = r^2 \in A$ and $rsr^2r^{-1} = sr^0 = s \in A$, so $r \in N_{D_8}(A)$. Because $N_{D_8}(A) \leqslant D_8$ contains r and s which generate D_8, we have $N_{D_8}(A) = D_8$.

2. Show that $Z(D_{2n}) = \{1\}$ if n is odd.

   We have $r^isr^jr^{-1} = sr^{-2i+j} = sr^j$ if and only if $-2i + j = j \mod n$, since $|r| = n$. This implies that n divides $2i$ and since n is odd, n divides i. So the only power of r commuting with an element of the form sr^j is $r^{kn} = 1$. Since every element of D_8 is either of the form r^i or of the form sr^i, it follows that the only element of D_{2n} which commutes with every other element is 1. So $Z(D_{2n}) = \{1\}$.

Problem 4 :

Let G be a group. For all $g \in G$, we define $f_g : G \to G$ by $f_g(x) := g \cdot x \cdot g^{-1}$.

1. Show that f_g is a group automorphism.

   Solution: Pick $x, y \in G$. We have $f_g(x) \cdot f_g(y) = g \cdot x \cdot g^{-1} \cdot g \cdot y \cdot g^{-1} = g \cdot x \cdot y \cdot g^{-1} = f_g(x \cdot y)$. So f_g is a group homomorphisme.

   We have $f_{g^{-1}}(f_g(x)) = g^{-1} \cdot g \cdot x \cdot g^{-1} \cdot g = x$ and $f_g(f_{g^{-1}}(x)) = g \cdot g^{-1} \cdot x \cdot g \cdot g^{-1} = x$ so f_g and $f_{g^{-1}}$ are inverse functions and f_g is bijective. So f_g is a bijective homomorphism from G to itself, i.e. an automorphism.

   One can also check injectiveity and surjectivity directly. If $f_g(x) = g \cdot x \cdot g^{-1} = g \cdot y \cdot g^{-1} = f_g(y)$, then, multiplying on the left by g^{-1} and on the right by g, we get that $x = y$. And since $f_g(g^{-1} \cdot x \cdot g) = g \cdot g^{-1} \cdot x \cdot g \cdot g^{-1} = x$, f_g is surjective.

2. Show that $\theta : g \mapsto f_g$ is a group homomorphism from G into $\mathrm{Aut}(G)$.

   Solution: Pick $g, h \in G$. We want to show that $\theta(g \cdot h) = f_{g \cdot h} = f_g \circ f_h = \theta(g) \circ \theta(h)$. Pick $x \in G$, we have $f_{g \cdot h}(x) = g \cdot h \cdot x \cdot (g \cdot h)^{-1} = g \cdot h \cdot x \cdot h^{-1} \cdot g^{-1} = g \cdot f_h(x) \cdot g^{-1} = f_g(f_h(x))$. We do have $f_{g \cdot h} = f_g \circ f_h$.

3. Show that $\ker(\theta) = Z(G)$

   Solution: We have that $g \in \ker(\theta)$ if and only if $\theta(g) = f_g = \mathrm{id}$, i.e. for all $x \in G$, $g \cdot x \cdot g^1 = f_g(x) = x$. So $\ker(\theta) = \{g \in G : \forall x \in G, g \cdot x \cdot g^1 = x\} = Z(G)$.