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

Solutions to the midterm (Lecture 003)

March 8th

Problem 1 (Translation action) :

1. Let us show that σ_g is injective. Assume $\sigma_g(i) = \sigma_g(j)$, then $g \cdot g_i = g \cdot g_j$ and thus $g_i = g_j$. It follows (because the g_i are all distinct), that $i = j$. So σ_g is an injection from $\{0, \ldots, m-1\}$ into itself. So it must be a bijection.

   Actually proving that σ_g is surjective is not very hard either. Let $i \in \{0, \ldots, m-1\}$, then there is some j such that $g_j = g^{-1} g_i$ and hence $\sigma_g(j) = i$.

   One can also directly prove that $\sigma_{g^{-1}}$ is the inverse of σ_g. Indeed $\sigma_g(\sigma_{g^{-1}}(i))$ is j such that $g_j = gg^{-1}g_i = g_i$ so $\sigma_g(\sigma_{g^{-1}}(i)) = i$ and $\sigma_{g^{-1}}(\sigma_g(i))$ is j such that $g_j = g^{-1}gg_i = g_i$ so $\sigma_{g^{-1}}(\sigma_g(i)) = i$.

2. For all $i \in \{0, \ldots, m-1\}$, $\sigma_g^k(i) = j$ such that $g_j = g^k g_i$. As $g^n = 1$, we have that $\sigma_g^n(i) = i$. Moreover if $0 \leqslant k < n$ and $\sigma_g^k(i) = i$ then $g^k g_i = g_i$, therefore $g^k = 1$ and $k = 0$ (as $0 \leqslant k < n$ and n is the order of g).

   We know that σ_g is a product of disjoint cycles. Let γ_j be those cycles. If i is in the support of γ_j, then $\gamma_j^k(i) = \sigma_g^k(i)$. Let n_j be the length of the cycle γ_j, then $\gamma_j^n(i) = i$ so $n_j \leqslant n$ and $\gamma_j^{n_j}(i) = i$ if and only if $n_j = n$ by the above. So each of the γ_j is an n-cycle.

3. The bijection σ_g does not have any fixed points, so each element of $\{0, \ldots, m-1\}$ is in the support of one of the n-cycles of the decomposition in disjoint cycles. So σ_g is the product of m/n disjoint n-cycles. The sign of an n-cycle is $(-1)^{n-1}$ and ε is a group homomorphism, it follows that $\varepsilon(\sigma_g) = ((-1)^{n-1})^{m/n} = (-1)^{(n-1)m/n}$.

Problem 2 (Groups of order 15) :
Let G be a group of order 15.

1. By Cauchy's theorem, as 3 and 5 are two primes diving $|G| = 15$, there exists $a, b \in G$ such that $|a| = 3$ and $|b| = 5$. Note that all the elementes in $\langle a \rangle$ except 1 have order 3 and that all the elementes in $\langle b \rangle$ except 1 have order 5. It follows that $\langle a \rangle \cap \langle b \rangle = \{1\}$. I particular, if $a^i b^j = a^k b^l$, then $a^{i-k} = b^{l-j}$ and hence $a^{i-k} = 1 = b^{l-j}$. It follows that $i = k \mod 3$ and $j = l \mod 5$, in particular the $a^i b^j$ for $0 \leqslant i < 3$ and $0 \leqslant j < 5$ are distinct. There are 15 of them and thus $G = \{a^i b^j : 0 \leqslant i < 3 \text{ and } 0 \leqslant j < 5\} = \langle a, b \rangle$.

2. The subgroup $\langle b \rangle$ has index $15/5 = 3$ in G. As 3 is the smallest prime dividing $|G|$, $\langle b \rangle$ is normal (we saw that in class). So $aba^{-1} = aba \in \langle b \rangle$.

3. By the previous question, we have $aba = b^j$ for some j. Then $b = a^3 ba^{-3} = a(a(aba^{-1})a^{-1})a^{-1} = a(ab^j a^{-1})a^{-1} = a(b^j)^j a^{-1} = ((b^j)^j)^j = b^{j^3}$ (because conjugation by a is a group homomorphism). If follows that $b = b^{j^3}$ and hence $j^3 - 1 = 0 \mod 5$. We have $1^3 = 1 \mod 5$, $2^3 = 3 \mod 5$, $3^3 = 2 \mod 5$ and $4^3 = 4 \mod 5$ so the only possible j is $j = 1 \mod 5$ and hence $aba^{-1} = b$.

4. If $aba^{-1} = b$ then $ab = ba$. As G is generated by a and b, it follows that G is Abelian (we have, by induction, $a^i b^j a^k b^l = a^i a^k b^j b^l = a^k b^l a^i b^j$). Moreover $(ab)^k = a^k b^k = 1$ if and only if $a^k = b^{-k}$ and hence $3|k$ and $5|k$ so $15|k$. So $|ab| = 15$ and G is cyclic of order 15. It follows that $G \cong \mathbb{Z}/15\mathbb{Z}$.

   Some of you also tried to construct an isomorphism directly, here is one that works: $\varphi(a^i b^j) = i5 + j3 \mod 15$. It is well defined because $(i + 3k)5 + (j + 5l)3 = i5 + j3 + (k + l)15 = ip + j2 \mod 15$. It is now easily seen to be a group homomorphism: $\varphi(a^i b^j a^k b^l) = \varphi(a^i a^k b^j b^l) = (i + k)5 + (j + l)3 = i5 + j3 + k5 + l3 = \varphi(a^i b^j) + \varphi(a^k b^l) \mod 15$. Moreover it is injective because if $i5 + j3 = 0 \mod 15$, then $15|i5 + j3$. In particular $3|i5+j3$ and thus $3|i$ and $5|i5+j3$ and thus $5|j$, so $a^j b^j = 1$. As $|G| = |\mathbb{Z}/15\mathbb{Z}| = 15$ is finite, φ is an isomorphism.