Silvain Rideau
1091 Evans

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

Solutions to the midterm (Lecture 002)

March 8th

Problem 1 (Cyclic groups of order p^2) :

1. Let $G = \langle x\rangle$. The element x^a generates G if and only if $\gcd(a, p^2) = 1$. The $a \in \{0, \dots p^2 - 1\}$ that are not coprime with p^2 are exactly those divisble by p, so these elements are $0, p, \dots, (p-1)p$. There are p of those and all the other generate G. There are $p^2 - p = p(p-1)$ of those.

2. Let $g \in G$ be an element of order p^2, then $\langle g\rangle$ is a cyclic subgroup of G of order p^2. Moreover, if H and K are of order p^2 and $g \in H \cap K$ has order p^2, then $\langle g\rangle \leqslant H \cap K \leqslant H$, K is a subgroup of order $p^2 = |H| = |K|$ and hence $H = \langle g\rangle = K$. It follows that each element of order p^2 is in one and exactly one cyclic subgroup of order p^2. Each of those groups contain $p(p-1)$ elements of order p^2 by the previous question, so $n = p(p-1)m$.

Problem 2 (Groups of order $2p$) :

1. By Cauchy's theorem, as 2 and p are two primes diving $|G| = 2p$, there exists a, $b \in G$ such that $|a| = 2$ and $|b| = p$. Note that all the elementes in $\langle a\rangle$ except 1 have order 2 and that all the elementes in $\langle b\rangle$ except 1 have order p. 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 $i = k \mod 2$ and $j = l \mod p$, in particular the $a^i b^j$ for $0 \leqslant i < 2$ and $0 \leqslant j < p$ are distinct. There are $2p$ of them and thus $G = \{a^i b^j : 0 \leqslant i < 2 \text{ and } 0 \leqslant j < p\} = \langle a, b\rangle$.

2. The subgroup $\langle b\rangle$ has index $2p/p = 2$ in G and hence it is normal (we saw that in class). So $aba^{-1} = aba \in \langle b\rangle$.

   In that cas it can actually be seen by hand quite easily. If $aba = ab^j$ then $a = b^{j-1}$, a contradiction. So $aba = b^j \in\rangle b\langle$ for some j.

3. By the previous question, we have $aba = b^j$ for some j. Then $b = a^2 ba^2 = a(aba)a = ab^j a = (b^j)^j$ (because conjugation by a is a group homomorphism). If follows that $b = b^{j^2}$ and hence $j^2 - 1 = 0 \mod p$, i.e. $p|j^2 - 1 = (j-1)(j+1)$. As p is prime, it follows that $p|j - 1$ or $p|j + 1$ and hence $j = 1 \mod p$ or $j = -1 \mod p$.

4. If $aba = b$ then $ab = ba^{-1} = ba$. 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 $2|k$ and $p|k$ so $2p|k$. So $|ab| = 2p$ and G is cyclic of order $2p$. It follows that $G \cong \mathbb{Z}/2p\mathbb{Z}$.

   Some of you also tried to construct an isomorphism directly, here is one that works: $\varphi(a^i b^j) = ip + j2 \mod 2p$. It is well defined because $(i + 2k)p + (j + pl)2 = ip + j2 + (k + l)2p = ip + j2 \mod 2p$. It is now easily seen to be a group homomorphism: $\varphi(a^i b^j a^k b^l) = \varphi(a^i a^k b^j b^l) = (i + k)p + (j + l)2 = ip + j2 + kp + l2 = \varphi(a^i b^j) + \varphi(a^k b^l) \mod 2p$. Moreover it is injective because if $ip + j2 = 0 \mod 2p$, then $2p|ip + j2$. In particular $2|ip+j2$ and thus $2|i$ and $p|ip+j2$ and thus $p|j$, so $a^j b^j = 1$. As $|G| = |\mathbb{Z}/2p\mathbb{Z}| = 2p$ is finite, φ is an isomorphism.

5. Let $\varphi(a^i b^j) = s^i r^j$ where $r \in D_{2p}$ is a rotation of order n and s is a symmetry. Then φ is well defined because $s^{i+2k} r^{j+pl} = s^i (s^2)^k r^j (r^p)^l = s^i r^j$. Moreover, φ is a homomorphism as $\varphi(a^i b^j a^k b^l) = \varphi(a^i a^k b^{(-1)^k j} b^l) = s^{i+k} r^{(-1)^k j + l} = s^i r^j s^k r^l = \varphi(a^i b^j) + \varphi(a^k b^l)$. Finally φ is a surjection because $\mathrm{Im}(\varphi) \leqslant D_{2n}$ contains $\varphi(a) = s$ and $\varphi(b) = r$ which generate D_{2p}. As $|G| = |D_{2p}| = 2p$, φ is an isomorhism.

   I agree it is tempting to just say that D_{2p} and G are presented by the same generators and relations and so are isomorphic, but we never actually proved that, so we have to do it by hand... Also we have not really proved that G is presented this way, we only proved that G has two generators with the right relations, but there could be more a priori (except there are none for cardinality reasons, but one should show it).