Silvain Rideau
1091 Evans

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

Solutions to the midterm

February 13th

Problem 1 :

1. Let $f: G \to H$ be a group homomorphism and $H_0 \leqslant H$. Show that $f^{-1}(H_0) \leqslant G$.

   Solution: Recall that $f^{-1}(H_0) := \{g \in G : f(g) \in H_0\}$. Since $f(1) = 1 \in H_0$, it follows that $1 \in f^{-1}(H_0)$. Moreover, for all $x, y \in f^{-1}(H_0)$, we have $f(x), f(y) \in H_0$ and $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1} \in H_0$ too since $H_0 \leqslant H$. It follows that $x \cdot y^{-1} \in f^{-1}(H_0)$ and hence that $f^{-1}(H_0) \leqslant G$.

2. Define what a cyclic group is and give an example of a cyclic group of every order (finite and infinite).

   Solution: A group G is cyclic if there exist $x \in G$ such that $G = \{x^n : n \in \mathbb{Z}\}$. The group $\mathbb{Z}$ is cyclic of infinite order and for any $n \in \mathbb{Z}_{>0}$, $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n.

Problem 2 :

Let G be a group and $x, y \in G$, we define $[x,y] = x \cdot y \cdot x^{-1} \cdot y^{-1}$ and $[G] := \{[x,y] : x, y \in G\}$.

1. Let $f: G \to H$ be a group homomorphism and assume H is Abelian. Show that $[G] \subseteq \ker(f)$.

   Solution: Recall that $\ker(f) := \{g \in G : f(g) = 1\}$. We want to show that for all $x,y \in G$, we have $f([x,y]) = 1$. But $f([x,y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = f(x)f(x)^{-1}f(y)f(y)^{-1} = 1$. The third equality holds because H is Abelian.

2. Show that G is Abelian if and only if $[G] = \{1\}$.

   Solution: If G is Abelian, then for all $x, y \in G$, $xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = 1$. So $[G] \subseteq \{1\}$. You can also see that by the previous question: $[G]$ is included in the kernel of the identity map which is $\{1\}$.

   Conversely, if $[G] = \{1\}$, then for all $x, y \in G$, $xyx^{-1}y^{-1} = 1$.Therefore $xyx^{-1} = y$ and $xy = yx$.

3. Show that $[D_{2n}] = \{r^{2i} : i \in \mathbb{Z}\}$.

   Solution: We have $r^i s r^{-i} s^{-1} = r^{2i} s s^{-1} = r^{2i} s s^{-1}$, so every element of the form r^{2i} is in $C(D_{2n})$. To conclude, we can now compute every possible $[x,y]$ to check that we only get r^{2i}. We have:

$$\begin{aligned}
(r^i s^k)(r^j s^l)(r^i s^k)^{-1}(r^j s^l)^{-1} &= r^i s^k r^j s^l s^{-k} r^{-i} s^{-l} r^{-j} \\
&= r^{i+(-1)^k j} s^{k+l-k-l} r^{(-1)^{-l}(-i)-j} \\
&= r^{i+(-1)^{l+1} i - j + (-1)^k j}.
\end{aligned}$$

   If $l = k = 0$, we get $1 = r^{2 \cdot 0}$. If $l = k = 1$, we get $r^{2(i-j)}$. If $l = 0$ and $k = 1$, we get r^{-2j} and if $l = 1$ and $k = 0$, we get r^{2i}. Any of these elements is of the form r^{2i} for some $i \in \mathbb{Z}$.

Problem 3 :
Let n, $m \in \mathbb{Z}_{>0}$ be coprime, G be a group of order mn, $a \in G$ have order n and $b \in G$ have order m.

1. Show that $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   Solution: Pick any $x \in \langle a \rangle \cap \langle b \rangle$. Then $\langle x \rangle \leqslant \langle a \rangle$ and $\langle x \rangle \leqslant \langle b \rangle$. By the classification of subgroups of cyclic groups, $|x|$ divides both $|a|$ and $|b|$. It follows that it divides $\gcd(|a|, |b|) = 1$. So $|x| = 1$ and $x = 1$. Conversely, $a^0 = 1 = b^0$ so $1 \in \langle a \rangle \cap \langle b \rangle$.

2. For all i_1, i_2, j_1 and $j_2 \in \mathbb{Z}$, show that $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$ if and only if $i_1 \equiv i_2 \mod n$ and $j_1 \equiv j_2 \mod m$.

   Solution: 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 $a^{i_1 - i_2} = 1 = b^{j_2 - j_1}$. Since $|a| = n$ and $a^{i_1} = a^{i_2}$, it follows that $i_1 \equiv i_2 \mod n$. Similarly $j_1 \equiv j_2 \mod n$.

   Conversely, if $i_1 \equiv i_2 \mod n$ and $j_1 \equiv j_2 \mod m$, then $a^{i_1} = a^{i_2}$ and $b^{j_1} = b^{j_2}$, so $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$.

3. Show that every elements of G is of the form $a^i b^j$ for some i, $j \in \mathbb{Z}$.

   Solution: Since G is a group, $\{a^i b^j : i \in \mathbb{Z} \text{ and } j \in \mathbb{Z}\} \subseteq G$. In particular, $|\{a^i b^j : i \in \mathbb{Z} \text{ and } j \in \mathbb{Z}\}| \leqslant |G| = mn$. Moreover, by the previous question, for all $0 \leqslant i < n$ and $0 \leqslant j < m$, the $a^i b^j$ are distinct. It follows that $|\{a^i b^j : i \in \mathbb{Z} \text{ and } j \in \mathbb{Z}\}| \geqslant mn = |G|$. So $|\{a^i b^j : i \in \mathbb{Z} \text{ and } j \in \mathbb{Z}\}| = mn$ and $\{a^i b^j : i \in \mathbb{Z} \text{ and } j \in \mathbb{Z}\} = G$.