Silvain Rideau
1091 Evans

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

Solutions to homework 4

Due October 2nd

Problem 1 :
Let $G \leqslant \mathbb{R}$.

1. Assume that for all $b \in \mathbb{R}_{>0}$, there exists $g \in G$ such that $0 < g < b$. Show that for all $x, y \in \mathbb{R}$ such that $x < y$, there is $g \in G$ such that $x < g < y$.

   Solution: By hypothesis, there exists $a \in G$ such that $0 < a < y - x$. Moreover, the sequence $(n \cdot a)_{n \in \mathbb{Z}_{\leqslant 0}}$ goes to infinity, so there exists $n \in \mathbb{Z}_{\leqslant 0}$ such that $n \cdot a \leqslant x < (n+1) \cdot a$. But because $a < y - x$, it follows that $(n+1) \cdot a < x + (y - x) = y$ and $(n+1) \cdot a \in G$.

2. (Harder) If $a := \inf\{g \in G : g > 0\} \neq 0$, show that $G = a\mathbb{Z}$.

   Solution: It follows from the hypothesis that there exists $b \in \mathbb{R}_{>0}$ such that for all $c \in G_{>0}$, $b < c$. In particular if $d < c \in G$ then $c - d \in G_{>0}$ and hence $b < c - d$. It follows that elements of G are at least b apart. Let $c \in G_{>0}$ be such that $c - a < b$ (this exists because $a = \inf\{g \in G : g > 0\}$). If $c \neq a$, there exists $d \in G_{>0}$ such that $a \leqslant d < c$, but then $c - d \leqslant c - a < b$, a contradiction. It follows that $a \in G$. Now pick any $c \in G$, there exists $n \in \mathbb{Z}$ such that $n \cdot a \leqslant c < (n+1) \cdot a$. It follows that $0 \leqslant c - n \cdot a < a$ and hence, by minimality of a, $c - n \cdot a = 0$ and hence $c \in a \cdot \mathbb{Z}$.

Problem 2 :

1. Show that $x \mapsto e^{2i\pi x}$ is group homomorphism from $\mathbb{R}$ to $\mathbb{C}^{\star}$.

   Solution: We have $e^{2i\pi(x+y)} = e^{2i\pi x + 2i\pi y} = e^{2i\pi x} \cdot e^{2i\pi y}$, so this is a group homomorphism.

2. Let $\mathbb{T} = \{x \in \mathbb{C} : |x| = 1\}$ (here $|x|$ denotes the absolute value). Show that $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

   Solution: Let $g\mathbb{R}/\mathbb{Z} \to \mathbb{T}$ be the map defined by $g(x + \mathbb{Z}) := e^{2i\pi x}$. Let us show that g is well defined: for all x, $y \in \mathbb{R}$, if $x + \mathbb{Z} = y + \mathbb{Z}$, then $y = x + k$ where $k \in \mathbb{Z}$ and $e^{2i\pi y} = e^{2i\pi(x+k)} = e^{2i\pi x} e^{2i\pi k} = e^{2i\pi x} \cdot 1^k = e^{2i\pi x}$. Let us now show that g is a group homomorphism: for all x, $y \in \mathbb{R}$, $g((x + \mathbb{Z}) + (y + \mathbb{Z})) = g((x + y) + \mathbb{Z}) = e^{2i\pi(x+y)} = e^{2i\pi x} e^{2i\pi y} = g(x + \mathbb{Z}) \cdot g(y + \mathbb{Z})$.

   Let us show also that g is surjective. Pick $x \in \mathbb{C}$ mid $|x| = 1$. Writing x in polar notation, $x = |x| e^{2i\pi\theta} = e^{2i\pi\theta} = g(\theta + \mathbb{Z})$ for some $\theta \in \mathbb{R}$. Finally, let us show that g is injective. Since g is a group homomorphism, it suffices to compute its kernel: $\ker(g) = \{x + \mathbb{Z} : g(x + \mathbb{Z}) = e^{2i\pi x} = 1\} = \mathbb{Z}$.

   Now that we know the first isomorphism theorem, we can also use it (note that we just reproved it in this particular instance above). Let f be the group homomorphism of the previous question, then $\mathbb{T}$ is its image and its kernel is $\{x \in \mathbb{R} : e^{2i\pi x} = 1\} = \mathbb{Z}$ so $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$.

3. Show that in $\mathbb{Q}/\mathbb{Z} \leqslant \mathbb{R}/\mathbb{Z}$ all elements have finite order but the order can be arbitrarily large.

   Solution: Let $a \in \mathbb{Q}$, then $a = p/q$ for some $p \in \mathbb{Z}$, $q \in Zz_{>0}$ and $q \cdot a = p \in Zz$ so $q \cdot (a\mathbb{Z}) = (q \cdot a)\mathbb{Z} = \mathbb{Z}$ (the first equality is a additive instance of the well-known equation we (almost) proved by induction for the iteration of coset multiplication). So the order of a is at most q. Also, if we assume that p and q are relatively prime (and we can), then $n \cdot p/q \in \mathbb{Z}$ if and only if $q|np$ and hence $q|n$, so q is the order of a and q can be arbitratily large.

4. Show that $\mathbb{Q}/\mathbb{Z} \cong \mu_\infty = \{x \in \mathbb{C} : x^n = 1 \text{ for some } n \in \mathbb{Z}_{>0}\} \leqslant \mathbb{T}$.

   Solution: The image of $\mathbb{Q}/\mathbb{Z}$ by the isomorphism between $\mathbb{R}/\mathbb{Z}$ and $\mathbb{T}$ is $X := \{e^{2i\pi p/q} : p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_{>0}\}$ so $\mathbb{Q}/\mathbb{Z} \cong X$. Let us show that $X = \mu_\infty$. We have $(e^{2i\pi p/q})^q = e^{2i\pi p} = 1$ so $X \subseteq \mu_\infty$. Concersely, let $x \in \mathbb{C}$ and $n \in \mathbb{Z}_{>0}$ be such that $x^n = 1$ so $|x|^n = 1$ and, as $|x| \in \mathbb{R}_{>0}$, $|x| = 1$, i.e. $x = e^{2i\pi t}$ for some $t \in \mathbb{R}$. As $x^n = 1$, we have $n \cdot t = m \in \mathbb{Z}$ so $t = m/n \in \mathbb{Q}$ and hence $X = \mu_\infty$.

Note that the group μ_∞ was called Z in the previous homework.

Problem 3 :
Let G be a group and $H \leqslant G$ such that $[G : H] = n < \infty$

1. Assume that $H \trianglelefteq G$, show that for all $g \in G$, $g^n \in H$.

   Solution: We have $gH \in G/H$ which is a group of order n, it follows that $g^n H = (gH)^n = H$ and therefore $g^n \in H$.

2. (Harder) Find a counterexample when H is not normal.

   Solution: Let $G = S_3$, $H = \langle(01)\rangle$ and $g = (12)$, then $[G : H] = 6/2 = 3$ and $g^3 = g \notin H$.

Problem 4 :
Let $n \in \mathbb{Z}$, $n \geqslant 3$ and $d|n$. Let r denote one of the rotations in D_{2n} and $H = \langle r^d \rangle$.

1. Show that H is a normal subgroup of D_{2n}.

   Solution: Every element of H is of the form r^{id} for some $i \in \mathbb{Z}$. We have $rr^{id}r^{-1} = r^{id} \in H$ so $r \in N_{D_{2n}}(H)$ and $sr^{id}s^{-1} = ssr^{-id} \in H$ so $s \in N_{D_{2n}}(H)$. As D_{2n} is generated by r and s, it follows that $N_{D_{2n}}(H) = D_{2n}$, i.e. $H \trianglelefteq D_{2n}$.

2. If $d = 1$, show that $D_{2n}/H \cong \mathbb{Z}/2\mathbb{Z}$.

   Solution: $D_{2n} = \langle r \rangle \cup s\langle r \rangle$ so these are two cosets of H in D_{2n}. The group law is given by $H \cdot H = H = ssH = sH \cdot sH$, $sH \cdot H = sH = H \cdot sH$. It is now easy to check that by sending H to $\overline{0}$ and sH to $\overline{1}$ we get an isomorphism between D_{2n}/H and $\mathbb{Z}/2\mathbb{Z}$.

   More conceptually, $|D_{2n}| = 2n$ and $|H| = n$ so, by Lagrange's theorem D_{2n}/H is an order 2 group, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

3. If $d = 2$ (in particular, n has to be even), $D_{2n}/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Solution: $D_{2n} = \langle r^2 \rangle \cup r\langle r^2 \rangle \cup s\langle r^2 \rangle \cup sr\langle r^2 \rangle$ so these are the fours cosets of H in D_{2n}. We can now check that for $i, j, k, l \in \{0, 1\}$, $s^i r^j H \cdot s^k r^l H = s^i r^j s^k r^l H = s^{i+k} r^{l+(-1)^k j} H$. But since $r^{(-1)^k j} r^j = r^0$ or r^{2j} depending on the parity of k, we have $r^{(-1)^k j} r^j \in H$ and hence $s^i r^j H \cdot s^k r^l H = s^{i+k} r^{j+l} H$. It is now easy to check that the map from D_{2n}/H to $(\mathbb{Z}/2\mathbb{Z})^2$ sending $r^i s^j$ to (i, j) is a group homomorphism.

4. If $d > 2$, $D_{2n}/H \cong D_{2d}$.

   Solution: Let r_d and s_d denote, respectively, the rotation and symmetry that generate D_{2d} (we will continue to denote by r and s those in D_{2n}). Let $\varphi(r^i s^j) = (r_d^i s_d^j)$. Let us check that this map is well defined. If $r^i s^j = r^k s^l$, then $r^{i-k} = s^{l-j}$ so $r^{i-k} = 1 = s^{l-j}$ and so $n | i - k$ and $2 | l - j$. In particular, $d | i - k$ so $r_d^{i-k} = 1 = s_d^{l-j}$ and $r_d^i s_d^j = r_d^k s_d^l$. Also, φ is a group homomorphism, indeed $\varphi(r^i s^j r^k s^l) = \varphi(r^{i-k} s^{j+l}) = r_d^{i-k} s_d^{j+l} = r_d^i s_d^j r_d^k s_d^l = \varphi(r^i s^j) \cdot \varphi(r^k s^l)$. It is clear that φ is onto and $\varphi(r^i s^j) = r_d^i s^j = 1$ if and only if $d | i$ and $2 | j$, i.e. $r^i s^j = r^i \in \langle r^d \rangle = H$. It now follows from the first isomorphism theorem that $D_{2n}/H = D_{2n}/\ker(\varphi) \cong \mathrm{Im}(\varphi) = D_{2d}$.