Homework 5

Jaden Wang

Problem (1)**.** (collab with Ari and Will): Let G be a finitely generated group with generators $\{g_1, \ldots, g_m\}$ and suppose $H \leq G$ with $[G : H] = n$ for some $n \in \mathbb{Z}^+$. Let the cosets of H in G be $\{eH, a_2H, \ldots, a_nH\}$ (note we choose $a_1 = e$). Since $g_i a_j$ must be in one of the cosets a_kH, we see that $g_i a_j = a_k^{ij} h_{ij}$ for some $h_{ij} \in H$. Moreover, for any given a_k and g_i, let a_j be the representative of the coset that $g_i^{-1}a_k$ is in, then $a_kH = g_i g_i^{-1} a_k H = g_i a_j H$. Hence for every g_i we have $g_i a_j = a_k^{ij} h_{ij}$ for some a_j. That is, a_j (and therefore h_{ij}) is determined solely by the choice of a_k and g_i.

Now I claim that $\{h_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ generates H. Since elements of H are words of generators of G, any $h \in H$ is a finite string of g_i. We wish to use h_{ij} to recover h. So we start from the left: if the first letter in h is g_i, then by using $e = a_1 \in H$, we determine an a_j and h_{ij}. This yields

$$h_{ij} = e_{ij} h_{ij} = g_i a_j$$

So we recover the first letter g_i with an additional a_j on the right. Now suppose the second letter is g_ℓ, then a_j and g_ℓ determine an a_k and $h_{\ell k}$. Thus

$$\begin{aligned} h_{ij} h_{\ell k} &= g_i a_j h_{\ell k} \\ &= g_i g_\ell a_k \end{aligned}$$

So we recover the second letter, with an a_k on the right. Repeating this process until we recover the entire string of h with an a_p on the right. That is,

$$h_{ij} h_{\ell k} \ldots h_{qp} = g_i g_\ell \ldots g_q a_p = h a_p$$

But since the LHS is in H and $h \in H$, we have that a_p is also in H. This forces $a_p = a_1 = e$ (otherwise it would be a representative of a coset not equal to H). Hence $h = h_{ij} h_{\ell k} \ldots h_{qp}$. That is, it is a product of generators of the form h_{ij} as desired.

Problem (2)**.** $270 = 2 \cdot 3^3 \cdot 5$. Thus we only need to consider the partition of 3 which yields three cases: $3, (2, 1), (1, 1, 1)$.

invariant factor	elementary divisor
Z_{270}	$Z_2 \times Z_{3^3} \times Z_5$
$Z_{90} \times \mathbb{Z}_3$	$Z_2 \times Z_{3^2} \times Z_5$
$Z_{30} \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$.

Problem (3)**.** There is no element of order 2 in cyclic groups of odd order by Lagrange and there is a unique element of order 2 in each cyclic group with even order. Since for any cyclic group with even order $Z_n = \langle g \rangle$, $o(g) = n$, so $o(g^\alpha) = 2$ implies that $g^\alpha = g^{-\alpha} \Rightarrow g^{2\alpha} = g^n = e$ (since $\alpha \neq 0$ as that would be order 1). So $\alpha = n/2$ which is unique. Hence we have an element of order 2 from each even cyclic group, yielding 3 in total. Their lcm order is also 2 so we have $2^3 - 1 = 7$ ways to construct elements of order 2 as we exclude the identity.

Problem (4)**.** Since G is finite, we can resort to dual group. Due to the isomorphisms, it suffices to find an injective map from $\mathrm{Hom}(G, U)$ to $\mathrm{Hom}(G, U)$ which would induce an injection from $G/H \to G$ by isomorphisms. There are two ways to do this.

(1) Let U denote the group of all roots of unity (or replace it with $\mathbb{C}^*$). Consider the map $i^* : \mathrm{Hom}(G/H, U) \to \mathrm{Hom}(G, U), f \mapsto f \circ \pi$, where $\pi : G \to G/H$ is the canonical projection map. Let $\phi : G \to U$ be the trivial homomorphism that maps everything to 1. By the universal property of quotient groups, this induces a homomorphism $\Phi : G/H \to U$ s.t. $\phi = \Phi \circ \pi$. If $H = G$ the problem is trivial so WLOG assume H is a proper subgroup. Then π is not the trivial map. This forces Φ to be the trivial map in $\mathrm{Hom}(G/H, U)$, which shows that $\ker i^*$ is trivial so i^* is injective. By the isomorphisms we get an injective map $i : G/H \to G$ so $G/H \cong \mathrm{im}\, i \leq G$.

$$\begin{tikzcd}
G/H \arrow[r, hook, "i"] \arrow[d, tail, two heads] \arrow[dr, phantom, "\circ"] & G \arrow[d, tail, two heads] \\
\mathrm{Hom}(G/H, U) \arrow[r, hook, "i^*"'] & \mathrm{Hom}(G, U)
\end{tikzcd}$$

(2) By viewing G as a $\mathbb{Z}$-module, recall that $\mathrm{Hom}(-, U)$ is a right-adjoint functor between the cateogry of $\mathsf{R\text{-}mod}$ so it preserves colimits including cokernel. Consider the short

exact sequence:

$$0 \to H \xrightarrow{i} G \xrightarrow{\pi} G/H \to 0.$$

Applying $\mathrm{Hom}(-, U)$ to the sequence yields an left-exact sequence

$$0 \to \mathrm{Hom}(G/H, U) \xrightarrow{i^*} \mathrm{Hom}(G, U) \to \mathrm{Hom}(H, U)$$

By exactness, $\ker i^* = \mathrm{im}\, 0 = 0$ so i^* is injective. This yields the $i : G/H \to G$ we seek.

If we omit finite (so we cannot use dual group isomorphisms), then consider $G = \mathbb{Z}$, all subgroups of G are of infinite order, but for $H = 2\mathbb{Z}$, $G/H \cong Z_2$ which has finite order so it cannot be isomorphic to a subgroup of G.

If we omit abelian (so we cannot use either quotient group universal property or left-exactness of $\mathrm{Hom}(-, U)$), then consider $G = S_3$ and $H = \{e, (1, 2)\}$. G/H is not a group as H is not a normal subgroup, so G/H clearly cannot be isomorphic to a subgroup.

Problem (5)**.**

(a) First we show that $\widehat{G}$ is a group. It contains the identity $1_{\widehat{G}} : g \mapsto 1$ and is clearly associative. Given $f, g \in \widehat{G}$, since $\mathbb{C}^*$ is abelian, $(f \cdot g)(xy) = f(xy)g(xy) = f(x)f(y)g(x)g(y) = f(x)g(x)f(y)g(x) = (f \cdot g)(x)(f \cdot g)(y)$ so it is closed under pointwise multiplication. The inverse of f is just $f^{-1} : x \mapsto \frac{1}{f(x)}$ which is well-defined as $0 \notin \mathbb{C}^*$. Commutativity is obvious as $\mathbb{C}^*$ is abelian.

(b) Since G is finite abelian, by FToFGAB, $G \cong \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$. We denote the order of each g_i by n_i. We wish to show that $G \cong \mathrm{Hom}(G, \mathbb{C}^*)$. Define $x_i : G \to \mathbb{C}^*, g_i \mapsto e^{i2\pi/n_i}, g_j \mapsto 1, j \neq i$. Notice that $x_i^{n_i} : g_i \mapsto e^{i2\pi n_i/n_i} = 1, g_j \mapsto$ so n_i is the smallest power that makes x_i the trivial homomorphism so $o(x_i) = n_i$. I claim that $\{x_i\}$ generates $\widehat{G}$. Given $f \in \mathrm{Hom}(G, \mathbb{C}^*)$, it suffices to specify where f maps each generator g_i. Since f is a homomorphism, the order of $f(g_i)$ must divide n_i. Thus f must map g_i to a root of unity, *i.e.* $f : g_i \mapsto (e^{i2\pi/n_i})^{d_i} = (x_i(g_i))^{d_i}$ where d_i is some divisor of n_i. It follows that

$$f = \prod_{i=1}^{n} x_i^{d_i}$$

where the product denotes pointwise multiplication. Thus $\{x_i\}$ generates $\widehat{G}$. Then map

$$\phi : G \to \widehat{G}, g_i \mapsto x_i$$

is thus a well-defined homomorphism as we map generators to generators of the same orders. Surjectivity follows from hitting all x_i. Suppose $\phi(g) = 1_{\widehat{G}}$ where $1_{\widehat{G}} : G \to U, g \mapsto 1$ is the trivial homomorphism, since ϕ maps all generators g_i to a non-trivial homomorphism, the kernel must be trivial. Thus ϕ is an isomorphism.

Problem (6)**.** Given $x, y \in R$, $x^2 = x$ and $y^2 = y$, then notice $-x = (-x)^2 = x^2 = x$. Moreover,

$$\begin{aligned} x + y = (x+y)^2 &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y \\ 0 &= xy + yx \\ 0 &= -xy + yx \\ xy &= yx \end{aligned}$$

So R is commutative.

Problem (7)**.**

(a) Clearly IJ is non-empty. It is closed under addition because sum of finite sums is still finite. It is closed under negation because I, J are. Given $x_1y_1 + \cdots + x_ky_k \in IJ$ and $r \in R$, since I is an ideal, any $rx_i \in I$, so

$$r(x_1y_1 + \cdots + x_ky_k) = (rx_1)y_1 + \cdots + (rx_k)y_k \in IJ$$

So this proves closure under multiplication as well and shows that IJ is an ideal. Since x_iy_i is both in I and J, viewed as a left-ideal and right ideal respectively, the sum is also in both. So $IJ \subseteq I \cap J$.

Let $R = \mathbb{Z}, I = \langle 2 \rangle, J = \langle 4 \rangle$. Then $I \cap J = J$ but $IJ = \{2r_1 4r_1' + 2r_2 4r_2' + \cdots + 2r_k 4r_k' : r_i, r_i' \in R\} = \langle 8 \rangle \neq \langle 4 \rangle = I \cap J$.

(b) Suppose $I + J = R$. Then given $s \in I \cap J$, given $r \in R$, we can write it as $r = x + y$, $x \in I, y \in J$. Then

$$sr = s(x + y) = sx + sy = xs + sy \in IJ$$

Since IJ is an ideal, $(sr)r^{-1} = s \in IJ$ and $I \cap J \subseteq IJ$ which yields equality.