Exercise 5

Yuval Paz

Thursday 15th February, 2024

Exercise 1.

Part 1.1.

Let $\varphi : \mathbb{Z}^2 \to \mathbb{Z} \times \mathbb{Z}_m$ defined as $\varphi(a, b) = (a - b, b \pmod m)$.

We have $(a-b, b \pmod m) + (x-y, y \pmod m) = (a-b+(x-y), (b \pmod m) + y \pmod m) \pmod m) = ((a+x) - (b+y), (b+y) \pmod m)$ so φ is an homomorphism.

Given $(x, y) \in \mathbb{Z} \times \mathbb{Z}_m$ we have $\varphi(x + y, y) = (x, y)$ so this is surjective.

If $\varphi(x, y) = e$ we have that $x = y$ and $y \equiv_m 0$, in particular $(x, y) = (nm, nm)$ for some integer n, hence $\ker(\varphi) = \langle (m, m) \rangle$

By the first iso-theorem we have that $\mathbb{Z}^2 / \langle (m, m) \rangle \cong \mathbb{Z} \times \mathbb{Z}_m$.

Part 1.2.

Let $\varphi : \mathbb{R}^2 \to S_1 \times S_1$ defined as $(x, y) \mapsto (\exp(2\pi x), \exp(2\pi y))$. Clearly this is a surjective homomorphism with kernel being the $\mathbb{Z}^2$, hence from the first iso-theorem the result follows.

Part 1.3.

We have that $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q} \cap [0, 1)$ where the latter is with addition mod 1. This can be seen using the homomorphism $x \mapsto x - \lfloor x \rfloor$.

Let $x \in \mathbb{Q} \cap [0, 1)$, we have that $x = \frac{a}{b}$ for $b \in \mathbb{N} \setminus \{0\}$, in particular $x^b = 0$, so the order of x is at most $b \leq \infty$.

If we replace $\mathbb{Q}$ with $\mathbb{R}$ we still have the quotient isomorphic to $[0, 1) \cap \mathbb{R} = [0, 1)$, but then the order of $\frac{1}{\pi}$ is not finite, as it would imply that π is rational.

Exercise 2.

Part 2.1.

Let k be the order of g, and n the order of gN.

We have that $g^k = e \implies (gN)^k = g^k N = eN = N = e_{G/N} \implies n | k$

Part 2.2.

We know that an order of an element divides the order of the group, so $n|[G:N]$, in particular $mn = [G:N]$ hence $g^{[G:N]}N = (gN)^{[G:N]} = e_{G/N} = N$.

From that $g^{[G:N]} \in N$ follows.

Exercise 3.

We know that $G/Z(G)$ must be either trivial, in which case $G = Z(G)$ and G is Abelian, or G, in this case $Z(G) = 1$, or $G/Z(G)$ has an order p, in which case it is cyclic hence G is Abelian.

We shall show that $Z(G)$ cannot be trivial, indeed if it was then we would get from the Conjugacy class equation that $p^2 = |G| = |Z(G)| + \sum \cdots$ where each term of the sum is an order of a quotient, hence p divides it. This gives us that p must divides $|Z(G)| \implies |Z(G)| \neq 1$.

Exercise 4.

Part 4.1.

We have that $ijk = -1$ so $k = -jjk = j(-j)k = jiijk = (ji)(ijk) = -ji \implies ji = -k$.

We have that $-kk = -(-1) = 1$, hence $ij = (-i)(-j) = (-i)^{-1}(-j)^{-1} = ((-j)(-i))^{-1} = (ji)^{-1} = (-k)^{-1} = k$.

Part 4.2.

In D_4 we have 6 elements of order 2, $e, \sigma^2, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$, but in $\mathbb{H}$ we only have 2, ± 1, the rest of order 4.

Part 4.3.

We know that $\pm 1 \in Z(\mathbb{H})$, and that $i, j \notin Z(\mathbb{H})$.

If k were in $Z(\mathbb{H})$ then we would get $kij = -1$, and a symmetric argument of what we did in 4.1 would give that $ki = -ik$, and k, i won't don't commute.

Therefore $Z(\mathbb{H}) = \{1, -1\}$.

Part 4.4.

We have at least the subgroups $1, \langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$.

Each of the latter 3 are of order 4 hence cannot be extended to a different proper subgroup, and the first 2 are subgroups of the latter 3, hence those are the only proper subgroups.

The first 2 subgroups are clearly normal as they are subgroups of the center, and the latter 3 are also normal because they have index 2.

Part 4.5.

We know that 1 is one of the conjugacy classes and that $\{-1\}$ is another, as $1, -1 \in Z(\mathbb{H})$.

We shall look at $\mathrm{Cl}(i)$, We have $jij^{-1} = -jij = -jk$, because $ijk = -1$ we have $jk = i$, hence $jij^{-1} = -i$. $kik^{-1} = -ijiij = ijj = -i$, so we get that $\mathrm{Cl}(i) = \{i, -i\}$.

We notice that $ijk = -1 \implies -jk = -i \implies -jki = 1 \implies jki = -1$, so from symmetry $kij = -1$ and $\mathrm{Cl}(k) = \{k, -k\}, \mathrm{Cl}(j) = \{j, -j\}$

Exercise 5.

We have that $D_5 = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4\}$.

We have that e is of order 1, $\sigma, \sigma^2, \sigma^3, \sigma^4$ of order 5, and $\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4$ of order 2.

Furthermore, if $\varphi : D_5 \to D_5$ is automorphism, it completely determined from $\varphi(\sigma), \varphi(\tau)$.

Because automorphism preserves order, it must sends σ to an element of order 5, and τ to an element of order 2.

Let $0 < r, t < 5$ such that $\varphi(\sigma) = \sigma^r$ and $\varphi(\tau) = \tau\sigma^t$, we shall show that this induces an automorphism and hence all possible functions of that form are automorphism and we shall achieve that $|\operatorname{Aut}(D_5)| = 20$.

We extend φ to the function $\varphi(e) = e, \varphi(\tau\sigma^j) = \tau\sigma^{jr+t \pmod 5}, \varphi(\sigma^i) = \sigma^{ir \pmod 5}$. The fact that φ preserve the group operation when multiplying σ^j with anything is almost by definition, so we shall only check $\varphi(\tau\sigma^j)\varphi(\tau\sigma^i) = \tau\sigma^{jr+t \pmod 5}\tau\sigma^{ir+t \pmod 5} = \sigma^{-jr-t \pmod 5}\sigma^{ir+t \pmod 5} = \sigma^{(i-j)r \pmod 5} = \varphi(\sigma^{i-j}) = \varphi(\tau\tau\sigma^{i-j}) = \varphi(\tau\sigma^j\tau\sigma^i)$