Exercise 2

Yuval Paz

Thursday 1st February, 2024

Exercise 1.

Part 1.1.

Let $a_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, a_y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in G$, then we have $a_x a_y = \begin{pmatrix} 1 \cdot 1 + x \cdot 0 & 1 \cdot y + x \cdot 1 \\ 0 \cdot 1 + 0 \cdot 1 & 0 \cdot y + 1 \cdot 1 \end{pmatrix} = a_{x+y} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$.

To see that $x \mapsto a_x$ is an isomorphism we need to show it is a bijection (which is obvious by the definition, alternatively, $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mapsto x$ is an inverse function, which exists iff the function is a bijection), that it sends $e_{\mathbb{F}^+}$ to $e_G = I_2$ (which is true because $e_{\mathbb{F}^+} = 0_{\mathbb{F}}$), and that it preserves the group operator, which is shown to be true in the starting sentence.

Part 1.2.

We will show that $x \mapsto \exp(x)$ is an isomorphism from $\mathbb{R}^+$ to $\mathbb{R}^\times_{>0}$.

Clearly $\exp(x+y) = \exp(x)\exp(y)$, and $\exp(0) = 1$, and it is a strictly monotonic continuous function with $\lim_{x\to-\infty}\exp(x) = 0, \lim_{x\to\infty}\exp(x) = \infty$, so it's injective range is $(0,\infty)$, hence bijective (to $\mathbb{R}^\times_{>0}$).

Part 1.3.

Let f defined as:

$$\begin{aligned} 1 &\overset{f}{\mapsto} (0,0) \\ 3 &\mapsto (0,1) \\ 5 &\mapsto (1,0) \\ 7 &\mapsto (1,1) \end{aligned}$$

This is clearly a bijection and it sends the identity to the identity.

We just need to check how $3, 5, 7$ interact under f (as 1 is sent to the identity)

$$\begin{aligned}
3, 5: &\quad f(7) = f(15) = f(3 \cdot 5) = f(3) + f(5) = (1, 1) \\
3, 7: &\quad f(5) = f(21) = f(3 \cdot 7) = f(3) + f(7) = (1, 0) \\
5, 7: &\quad f(3) = f(35) = f(5 \cdot 7) = f(5) + f(7) = (0, 1)
\end{aligned}$$

Because the groups are Abelian, we are done.

Part 1.4.

The center $Z(S_4)$ is trivial, as if $p \in S_4$ moves $i \mapsto j$, and $k, \ell \neq i, j$ then $j = p \circ (i, k)(k)$ but $p(k)$ is one of i, k, ℓ, non of which (i, k) sends to j.

On the other hand we saw that $Z(D_n)$ is not trivial for even n.

Part 1.5.

Every element of $\mathbb{C}^\times$ has a root, but not every element of $\mathbb{R}^\times$ has a root.

Part 1.6. *Bonus*

Let $(p_i)_{i \in \omega}$ be the prime numbers, and define $f : \{p_i\}_{i \in \omega} \to \mathbb{Z}[x]^+$ defined by $f(p_i) = x^i$.

This function can be extend into F a function on all of $\mathbb{Q}^\times_{>0}$ using $F(xy) = F(x) + F(y)$ and $F(p_i) = f(p_i)$.

This function is surjective as $z_0 \cdot x^i + z_1 \cdot x^j = F(p_i^{z_0} p_j^{z_1})$, it is injective by the fundamental theorem of arithmetic, and it respects the operator by definition.

Exercise 2.

Part 2.1.

Let $H = K \leq D_3$ be the subgroups $\{e, \tau\}$ (this is a group as $\tau^2 = e$), in this case $HK = H$ is a group.

Let $K = \{e, \tau\sigma\}$ (this is a subgroup as $\tau\sigma\tau\sigma = e$), and let H as before, then $HK = \{e, \sigma, \tau, \tau\sigma\}$, but this is not a group as $\sigma^2 \notin HK$.

Part 2.2.

Assume HK is a group, let $h \in H, k \in K$, then $h^{-1}k^{-1} \in HK$, then $kh = (h^{-1}k^{-1})^{-1} \in HK$ so $KH \subseteq HK$.

Now we want to show that $hk \in KH$, but from before $k^{-1}h^{-1} \in HK$ so $k^{-1}h^{-1} = pq$ for $p \in H, q \in K$ which implies $hk = (pq)^{-1} = q^{-1}p^{-1} \in KH$.

Now assume $HK = KH$, clearly $e \in HK$ and HK is closed under $(—)^{-1}$, let $ab, xy \in HK$ with $a, y \in H, b, x \in K$, we have that $abx \in HK$, so it is in KH and equal to $tr, t \in K, r \in H$, which gives $abxy = try \in KH = HK$.

Part 2.3.

We have that for $ab \in HK$ and $x \in H \cap K$ (hence x^{-1} is in there) we have $ab = axx^{-1}b$, and because multiplication by a and multiplication by b are bijections we don't have repetition.

For each $g \in HK$ let $h_g \in H, k_g \in K$ such that $h_g k_g = g$.

Let $hk = g$, so $hk = h_g k_g \implies h_g^{-1}h = k^{-1}k_g \in H \cap K$ and $(h_g^{-1}h)h_g = h$ and $k = k_g(k^{-1}k_g)^{-1} = k_g(h_g^{-1}h)^{-1}$.

So the function $(h, k) \mapsto (hk, h_g^{-1}h)$ is a bijection from $|H||K|$ to $|HK||H \cap K|$

Part 2.4.

We have that $|HK| \leq |G|$ so $|G| < (1 + \sqrt{|G|})^2 \leq |H||K| = |HK||H \cap K| \leq |G||H \cap K| \implies |H \cap K| > 1$

Part 2.5.

Let $H < G$ be a subgroup of order q and let $e \neq h \in H$, if $\langle h \rangle \neq H$ then the order of h will divide q but not be $1, q$, the same argument gives that H has non non-trivial subgroups. If $K < G$ is another such group, it is generated from $k \in K$.

From the previous part we have that for some $n, m < q$ we have $k^n = h^m \implies k = h^{m-n} \implies k \in \langle h \rangle \implies \langle k \rangle \leq \langle h \rangle \implies \langle k \rangle = \langle h \rangle$

Exercise 3.

Part 3.1.

- It is faithful: given $g \in S_n$ if $gx = x$ for all $x \in [n]$ then it is the identity function by definition.
- It is transitive: given $x, y \in [n]$ we have that $(x, y)x = y$.
- It is not free for $n \neq 2$: $(1, 2)$ moves 1 and fixes 3
- The orbit $O(1), O(n)$ are both n, as for every $k \in n$ we have $(1, k), (k, n)$ that witness that k is in the orbit.
- The stabilizer $G_1 = S_{[n]\setminus\{1\}}$ and $G_n = S_{[n-1]} = S_{n-1}$.
- The size of the orbits is n and the size of the stabilizers is $|S_{n-1}| = (n-1)! = n!/n = |S_n|/|O(n)|$

Part 3.2.

- It is faithful: given $g \neq id$, and $gk = j$ for $k \neq j$, then $g\{k, j+1\} = \{j, g(j+1)\} \neq \{k, j+1\}$
- It is transitive: given $\{a, b\}, \{c, d\}$, then $(a, c)(b, d)\{a, b\} = \{c, d\}$ where $d \neq a$, if they are equal use (b, c) instead.

- It is never free: $(1,2)\{1,2\} = \{1,2\}$
- $O(\{1,n\}) = [[n]]^2$ from transitivity
- $G_{\{1,n\}} = \{g \in G \mid \{g1, gn\} = \{1,n\}\} = S_{[n]\setminus\{1,n\}} \cup \{g \circ (1,n) \mid g \in S_{[n]\setminus\{1,n\}}\}$
- $|O(\{1,n\})| = |[[n]]^2| = \binom{n}{2} = n \cdot (n-1)/2$
- $|G_{\{1,n\}}| = (n-2)! + (n-2)! = 2(n-2)! = |G|/|O(\{1,n\})|$

Part 3.3.

- It is faithful: Each vertex can any other vertex using only rotation
- It is transitive: It is a subgroup of a transitive group S_n
- It is not free: reflection that passes through a vertex will fix those and only those vertex, so it is not the identity and has fix points.
- Like the previous examples, the orbit is the whole domain of the group action as the action is transitive.
- The stabilizer of a vertex is only the identity and the reflection that passes through this vertex
- The cardinality of the orbit is n
- The order of the stabilizer is 2

Exercise 4.

Let n be even.

Every element is of the form $e, \sigma^k, \tau\sigma^k$.

We shall calculate the conjugacy classes of σ^k first: $\sigma^p\sigma^k\sigma^{-p} = \sigma^{p+k-p} = \sigma^k$, $\tau\sigma^p\sigma^k\sigma^{-p}\tau = \tau\sigma^k\tau = \tau\tau\sigma^{n-k} = \sigma^{n-k}$, so the conjugacy class is $\{\sigma^k, \sigma^{n-k}\}$.

Moving on to τ: $\sigma^p\tau\sigma^{-p} = \tau\sigma^{-2p} = \tau\sigma^{n-2p}$, $\tau\sigma^p\tau\sigma^{-p}\tau = \sigma^{n-2p}\tau = \tau\sigma^{2p}$, so the conjugacy class of τ is $\tau\sigma^{2k}$ $(0 \leq k < n/2)$. (We use the fact that n is even as we claim that $2p \pmod{n} = 2k$ for $p < n$)

Lastly, $\tau\sigma$: $\sigma^p\tau\sigma\sigma^{-p} = \tau\sigma^{1-2p} = \tau\sigma^{n-2p+1}$, $\tau\sigma^p\tau\sigma\sigma^{-p}\tau = \sigma^{n-2p+1}\tau = \tau\sigma^{2p-1}$, so the conjugacy class of τ is $\tau\sigma^{2k+1}$ $(0 \leq k < n/2)$. (We use the fact that n is even as we claim that $2p+1 \pmod{n} = 2k+1$ for $p < n$)

For n odd, the conjugacy classes we calculated for σ^k don't change, but now $2k$ for $p < n$ will generate all of the values between 0 and $n-1$, so the conjugacy class of τ is $\tau\sigma^k$ (for $0 \leq k < n$)