Exercise 2

Holo

Friday 19th January, 2024

Exercise 1.

Part 1.1.

Lets remember that a cycle is just a function f for a finite set X to itself such that $\mathrm{Supp}(f) = \{f^{(n)}(a)\}_{0 \leq n < |X|}$ for any $a \in \mathrm{Supp}(f)$.

To see that the 2-cycles, let's call this set C_2, generate the cycles (that we already saw generate the permutation group) we first note that $e \in \langle C_2 \rangle$ because if $a, b \in X$ then $(a, b)(b, a) = e$. Now, let f be a non-identity cycle, we know that $\mathrm{Supp}(f) \neq \emptyset$, let a be such witness. Let f_i be $(f^i(a), f^{i+1}(a))$, because X is finite we must have $\{f_i\}_{i \in \omega}$ finite and clearly we have $f = f_0 \circ f_1 \circ \cdots \circ f_{|\{f_i\}_{i \in \omega}|-1}$.

Part 1.2.

Let the set of $(i, i+1)$ be F_2. To see that it generates S_n we will show that F_2 generates C_2.

Because $(a, b)^{-1} = (b, a)$ we may will always assume that when we write (a, b) we have $a < b$, and because if (g_i) is a sequence from F_2 that generates $(c - a, b - a)$ we can shift all of g_i by a to get (c, b) it is enough to show that we generate $(1, k)$ to prove we generate (a, b) for all a, b with $b - a = k - 1$.

We will use induction on k in $(1, k)$, starting with 2. The base case is trivial so lets assume we generate $(1, k)$ and show $(1, k + 1)$.

We can compose $(1, k)$ with $(k, k+1)$ and then again with $(1, k)$ to get $g = (1, k)(k, k+1)(1, k)$. Clearly $g(i) = i$ for $i \notin \{1, k, k+1\}$, $g(k) = (1, k)(k, k+1)(1, k)k = (1, k)(k, k+1)1 = (1, k)1 = k$, $g(1) = (1, k)(k, k+1)(1, k)1 = (1, k)(k, k+1)k = (1, k)k+1 = k+1$ and $g(k+1) = (1, k)(k, k+1)(1, k)k+1 = (1, k)(k, k+1)k+1 = (1, k)k = 1$, in other words $g = (1, k+1)$ and we are done.

Part 1.3.

First we notice that $(1, \ldots, n)k \equiv k + 1 \pmod{n}$, so let $1 < p < n$ and look at $h = (1, \ldots, n)^{(p-1)}(1, 2)(1, \ldots, n)^{(-(p-1))}$. Plugin the values of $p, p+1$ and $k \notin \{p, p+1\}$ we see that $h = (p, p+1)$.

Exercise 2.

Part 2.1.

Clearly if a is a multiply of $\operatorname{lcm}(d_1, d_2)$ then it is a multiply of both d_1, d_2, in other words $\langle \operatorname{lcm}(d_1, d_2)\rangle \subseteq \langle d_1\rangle \cap \langle d_2\rangle$.

To see the other direction let $x \in \langle d_1\rangle \cap \langle d_2\rangle$, but this means that x is a multiply of both d_1 and d_2, then $x = k \operatorname{lcm}(d_1, d_2) + r, r < \operatorname{lcm}(d_1, d_2)$, if $r \neq 0$ then it divides both d_1, d_2, contradiction to the minimality, so $x = k \operatorname{lcm}(d_1, d_2) \implies x \in \langle \operatorname{lcm}(d_1, d_2)\rangle$

Part 2.2.

Assume $\operatorname{lcm}(|g|, |h|) = k|gh| + r, r < |gh|$ and look at $(gh)^{\operatorname{lcm}(|g|,|h|)} = (gh)^{k|gh|+r} = (gh)^r$.

But $(gh)^{\operatorname{lcm}(|g|,|h|)} = g^{\operatorname{lcm}(|g|,|h|)}h^{\operatorname{lcm}(|g|,|h|)} = 0$, so r must be divisible by both $|g|$ and $|h|$, which contradiction to the minimality of $\operatorname{lcm}(|g|, |h|)$ unless $r = 0$.

Part 2.3.

We have that $C = AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, with $C^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

On the other hand, $A^4 = I_2$ and $B^6 = I_2$, in particular from the previous part, if $AB = BA$ then $(AB)^{\operatorname{lcm}(4,6)} = C^{\operatorname{lcm}(4,6)} = I_2 \neq \begin{bmatrix} 1 & \operatorname{lcm}(4,6) \\ 0 & 1 \end{bmatrix}$

Part 2.4.

It is enough to show that for 2 disjoint cycles d, d' we have that $|dd'| = \operatorname{lcm}(|d|, |d'|)$.

If $d^{|dd'|}$ or $d'^{|dd'|}$ is the identity we are done (as it implies that the other is the identity, and from the previous parts we get $|dd'| = \operatorname{lcm}(|d|, |d'|)$), but then $d^{|dd'|}, d'^{|dd'|}$ are 2 disjoint nontrivial cycles, in particular $(dd')^{|dd'|} = d^{|dd'|}d'^{|dd'|} \neq e$, contradiction.

Exercise 3.

Part 3.1.

If $|g| = n$ then the function $\mathbb{Z}_n \to G : k \mapsto g^k$ is clearly an isomorphism.

Similarly, the same function with domain $\mathbb{Z}$ will be an isomorphism for $|g| = \infty$.

Part 3.2.

$(1, 1), (1, 1)+(1, 1) = (0, 2), (0, 2)+(1, 1) = (1, 0), (1, 0)+(1, 1) = (0, 1), (0, 1)+(1, 1) = (1, 2), (1, 2) + (1, 1) = (0, 0), (0, 0) + (1, 1) = (1, 1)$ so $\langle(1, 1)\rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$ and $|(1, 1)| = 6$, so from the previous part they are isomorphic.

Part 3.3.

$(a, b) + (a, b) = (0, 0), (0, 0) + (a, b) = (a, b)$ for all (a, b), so $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Exercise 4.

If $H, K \neq H \cup K$, there exists $h \in H \setminus K, k \in K \setminus H$. If $hk \in H \cup K$ then it is in one of H, K, which is clearly a contradiction as we will have $h^{-1}hk \in H$ or $hkk^{-1} \in K$.

Exercise 5.

Part 5.1.

If $C \in \mathrm{SL}_n(\mathbb{F}_p)$ then clearly $\det(AC) = \det(A)\det(C) = \det(A)$ hence we have $A \cdot \mathrm{SL}_n(\mathbb{F}_p) \subseteq \{B \in \mathrm{GL}_n(\mathbb{F}_p) \mid \det(B) = \det(A)\}$.

Take B with $\det(B) = \det(A)$, then $\det(A^{-1}B) = \det(A^{-1})\det(B) = \det(A)^{-1}\det(B) = \det(B)^{-1}\det(B) = 1$, hence $A^{-1}B \in \mathrm{SL}_n(\mathbb{F}_p)$.

Part 5.2.

For each $k \in [1, p]$ there exists a matrix A_k with determinate k, all of which are in $\mathrm{GL}_n(\mathbb{F}_p)$ and those matrices bijects to $\mathrm{GL}_n(\mathbb{F}_p)/\mathrm{SL}_n(\mathbb{F}_p)$ by a natural map, composing $k \mapsto A_k \mapsto A_k \mathrm{SL}_n(\mathbb{F}_n)$ will finish the proof.

Exercise 6.

Part 6.1.

First we will observe that $\sigma^{-1} = \sigma^{n-1}, \tau^{-1} = \tau$.

We will prove by induction on the length of the term that every $x \in D_n$ is either of the form σ^k or $\tau\sigma^k$.

To do this we notice that $\sigma\tau\sigma\tau = e \implies \sigma\tau = \tau^{-1}\sigma^{-1} = \tau\sigma^{n-1}$, which easily implies that $\sigma^{-1}\tau = \tau\sigma^{(n-1)^2} = \tau\sigma$. Indeed we can define an embedding $j : D_n \to S_n$ with $j(\tau) = (x \mapsto n-1-x)$ and $j(\sigma) = (x \mapsto x+1 \pmod n)$, and then

$$\begin{aligned} j(\sigma\tau\sigma\tau) &= x \mapsto ((n-1-((n-1-x)+1))+1 \pmod n) \\ &= x \mapsto ((n-1-(n-x))+1 \pmod n) \\ &= x \mapsto ((x-1)+1 \pmod n) \\ &= x \mapsto x \\ &= j(e) \end{aligned}$$

Now given $x \in D_n$ a term of length $p > 2$, it is of the form gh for $g \in \{\tau, \sigma\}$ and h of length $p-1$, by the induction hypothesis h is either of the form σ^k, in which case we are done, or of the form $\tau\sigma^k$. So $x = g(\tau\sigma^k) = (g\tau)\sigma^k$, if $g = \tau$ we are done, otherwise $x = (\tau\sigma^{n-1})\sigma^k = \tau\sigma^{k-1}$.

Part 6.2.

Let $g, h \in D_n$, let's also assume neither of them is e.

Let $g = \sigma^p, h = \sigma^q$, in this case $gh = \sigma^{p+q \pmod n}$.

Let $g = \tau\sigma^p, h = \sigma^q$, in this case $gh = \tau\sigma^p\sigma^q = \tau\sigma^{p+q \pmod n}$.

Let $g = \sigma^p, h = \tau\sigma^q$, in this case $gh = \sigma^p\tau\sigma^q$, from the observation we did in the previous part we can repeatedly move τ back using the identity $\sigma\tau = \tau\sigma^{-1}$, so $\sigma^p\tau = \tau\sigma^{-p} \implies gh = \sigma^p\tau\sigma^q = \tau\sigma^{q-p \pmod n}$

Let $g = \tau\sigma^p, h = \tau\sigma^q$, in this case $gh = \tau\sigma^p\tau\sigma^q = \tau^2\sigma^{q-p \pmod n} = \sigma^{q-p \pmod n}$

Part 6.3.

From the previous part we can find for all $g = \sigma^k$ an h such that $gh = \tau^i \sigma^{1-k}, hg = \tau^i \sigma^{1+k}$, which are equal only for $k = n/2$. ($i \in \{0, 1\}$)

Similarly for $g = \tau\sigma^k$ we can find h such that $gh = \tau^i \sigma^{k-1}, hg = \tau^i \sigma^{k+1}$, which are never equal (unless $n = 2, k = 1$, in which case $\tau\sigma = e$).

So all we need to check is $\sigma^{n/2}$, and quickly plugging it in the equations from the previous part we can see it works.