Math 100A - Fall 2019 - Midterm II

Problem 1.

Let G denote the cyclic group of order 20, and let g be a generator.

(i) Write down, in terms of g, all other generators of G.
(ii) List all automorphisms $f : G \to G$.
(iii) List all subgroups of G.
(iv) List all elements of G of order 4.

`Solution:`

(i) *We showed in class that all generators of G are of the form g^k with $\gcd(k, 20) = 1$ and $0 \leq k < 20$. In our case, these are*

$$g, g^3, g^7, g^9, g^{11}, g^{13}, g^{17}, g^{19}.$$

(ii) *There are exactly 8 automorphisms of G, corresponding to mapping g to one of the above generators. We obtain the following automorphisms*

$$f_1(x) = x,\ \ f_3(x) = x^3,\ \ f_7(x) = x^7,\ \ f_9(x) = x^9,$$
$$f_{11}(x) = x^{11},\ \ f_{13}(x) = x^{13},\ \ f_{17}(x) = x^{17},\ \ f_{19}(x) = x^{19}.$$

(iii) *For each divisor k of 20 we have a unique subgroup of order k generated by $g^{\frac{20}{k}}$. We obtain 6 subgroups*

$$H_1 = \langle g^{20} \rangle = \{1\},\ H_2 = \langle g^{10} \rangle\ \ H_4 = \langle g^5 \rangle,\ H_5 = \langle g^4 \rangle,\ H_{10} = \langle g^2 \rangle,\ H_{20} = \langle g \rangle.$$

(iv) *The generator g has order 20 by hypothesis. Let g^k be an element of order 4 with $0 \leq k < 20$. By a theorem in class,*

$$o(g^k) = \frac{20}{\gcd(k, 20)} = 4 \iff \gcd(k, 20) = 5.$$

This yields the values $k = 5, k = 15$ so the only elements of order 4 are g^5, g^{15}.

Problem 2.

Let $f : G \to H$ be a group homomorphism, and let $K = \text{Ker } f = \{g : f(g) = 1\}$. We have seen in class that K is a subgroup.

(i) Show that K is a subgroup of G.
(ii) Prove that if $g \in G$ then $gKg^{-1} \subset K$.
(iii) Conclude that K is a normal subgroup of G.
(iv) Let G be the group of 2×2 invertible matrices with real entries. Give an example of a normal H subgroup of G, $H \neq \{1\}$ and $H \neq G$.

`Solution:`

(i) *Let $x, y \in K$. We show $xy^{-1} \in K$. This proves K is a subgroup.*
Since $x, y \in K$, we have

$$f(x) = 1, f(y) = 1.$$

By the properties of homomorphisms we have

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1 \cdot 1^{-1} = 1.$$

This shows that $xy^{-1} \in K$, as needed.

(ii) *We show $gKg^{-1} \subset K$. Let*

$$x \in gKg^{-1} \implies x = gkg^{-1} \text{ for some } k \in K.$$

Then $f(k) = 1$. We compute

$$f(x) = f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(k)f(g)^{-1} = f(g)f(g)^{-1} = 1.$$

Thus $x \in K$, completing the proof.

(iii) *Since g is arbitrary, we can replace g by g^{-1} in part (ii) thus obtaining*

$$g^{-1}Kg \subset K.$$

Multiplying to the left by g and the right by g^{-1} we obtain

$$K = g(g^{-1}Kg)g^{-1} \subset gKg^{-1}.$$

In part (ii) we showed the opposite inclusion. Therefore $gKg^{-1} = K$ for all $g \in G$, so K is normal.

(iv) *Let $G' = \mathbb{R} \setminus \{0\}$. This is a group under multiplication. Let*

$$f : G \to G', \ A \mapsto \det A.$$

This is a homomorphism as shown in class

$$f(AB) = \det(AB) = \det A \cdot \det B = f(A)f(B).$$

The kernel of $H = Ker\ f$ is the group of 2×2 matrices with determinant 1. This group was denoted by $SL_2(\mathbb{R})$. Clearly $H \neq \{1\}$ and $H \neq G$. By part (iii), H is normal.

Problem 3.

Let $G = \langle g \rangle$ and $H = \langle h \rangle$ be cyclic groups of orders m and n.

(i) If $\gcd(m, n) = 1$, show that $(g, h) \in G \times H$ is an element of order mn in $G \times H$. Conclude that $G \times H$ is also cyclic.

(ii) If $\gcd(m, n) = d \neq 1$ show that $G \times H$ is not cyclic.

`Solution:`

(i) *As shown in class, for a cyclic group we have* $|G| = o(g)$. *Thus* $o(g) = m$. *Similarly* $o(h) = n$. *In particular*

$$g^m = 1,\ h^n = 1.$$

Consequently,

$$g^{mn} = (g^m)^n = 1^n = 1$$

$$h^{mn} = (h^n)^m = 1.$$

Therefore

$$(g, h)^{mn} = (g^{mn}, h^{mn}) = (1, 1).$$

Note that the pair $(1, 1)$ *serves as identity in* $G \times H$. *In particular*

$$o((g, h))|mn.$$

Conversely, we show that

$$mn|o((g, h))$$

proving therefore that $o((g, h)) = mn$.

Indeed, let (g, h) *have order* N. *Then*

$$(g, h)^N = (1, 1) \implies (g^N, h^N) = (1, 1) \implies g^N = 1,\ h^N = 1.$$

Since

$$g^N = 1 \implies o(g)|N \implies m|N$$

and similarly

$$h^N = 1 \implies o(h)|N \implies n|N.$$

Since $\gcd(m, n) = 1$ *it follows* $mn|N$ *as claimed.*

We have shown that (g, h) *has order* mn. *Thus* $\langle (g, h) \rangle$ *is a subgroup of* $G \times H$ *of cardinality* $o((g, h)) = mn$. *But* $G \times H$ *also has* mn *elements. Thus we must have equality*

$$G \times H = \langle (g, h) \rangle,$$

also proving $G \times H$ *is cyclic.*

(ii) *If* $d = \gcd(m, n) \neq 1$, *we claim* $G \times H$ *has no element of order* mn *so in particular it cannot be cyclic. (For a cyclic group, the generator has order the size of the group, namely* $mn = |G \times H|$ *in our case.)*

Indeed, if $x \in G \times H$ *we claim*

$$x^{\frac{mn}{d}} = (1, 1)$$

so that $o(x) \leq \frac{mn}{d} < mn$. *To this end, write* $x = (a, b)$ *where* $a \in G$ *and* $b \in H$. *Write*

$$a = g^k, \ b = h^\ell.$$

Thus

$$a^{\frac{mn}{d}} = g^{\frac{kmn}{d}} = (g^m)^{\frac{n}{d} \cdot k} = 1.$$

Here, we used that n/d *is an integer and* $g^m = 1$. *Similarly*

$$b^{\frac{mn}{d}} = 1.$$

Thus

$$x^{\frac{mn}{d}} = (a^{\frac{mn}{d}}, b^{\frac{mn}{d}}) = (1, 1).$$

Problem 4.

(i) Show that if $\sigma \in S_n$ satisfies $\sigma^3 = \epsilon$, then σ is a product of disjoint cycles of length 3.

(ii) Let G be a group. For each $a \in G$, let

$$\sigma_a : G \to G, \; \sigma_a(g) = aga^{-1}$$

be the associated inner automorphism. Let

$$f : G \to \mathrm{Inn}(G), \; a \mapsto \sigma_a.$$

We have seen in class that f is a homomorphism. Show that the kernel of f equals the center $Z(G)$

(iii) For each $n \geq 3$, show that $\mathrm{Aut}(S_n)$ contains an element of order exactly 3.

`Solution:`

(i) *Since $\sigma^3 = \epsilon$, if follows that the order of σ divides 3. Write σ as product of disjoint cycles of lengths $n_1, \ldots, n_r$. Without loss of generality, we assume $n_i > 1$ since cycles of length 1 are just the identity. The order of σ is*

$$lcm[n_1, \ldots, n_r].$$

Thus

$$lcm[n_1, \ldots, n_r] | 3 \implies n_i | 3 \implies n_i = 3.$$

Thus σ is product of disjoint cycles of length 3.

(ii) *If $a \in Ker\ f$ we have*

$$\sigma_a = \mathbf{1} \iff \sigma_a(g) = g \iff aga^{-1} = g \iff ag = ga$$

for all $g \in G$. Thus $a \in Z(G)$ by definition.

(iii) *Let $\gamma = (1\,2\,3)$. We know $\gamma^3 = \epsilon$. We set*

$$f_\gamma : S_n \to S_n, \; f_\gamma(g) = \gamma g \gamma^{-1}.$$

Thus f_γ is an inner automorphism. We have seen in class that the composition of inner automorphisms is an inner automorphism corresponding to the composition in S_n. That is

$$f_\gamma \circ f_\gamma \circ f_\gamma = f_{\gamma^3} = f_\epsilon = \mathbf{1}.$$

Thus f_γ has order dividing 3 in the group $Aut(S_n)$ (the group law is composition.)

We claim f_γ cannot have order 1, so the order must be 3. If f_γ had order 1, then $f_\gamma = \mathbf{1}$. However for $g = (12)$ we have

$$f_\gamma(g) = \mu g \mu^{-1} = (123)(12)(132) = (23) \neq \tau.$$

This is not the only possible example.

Extra credit.

Find all subgroups of $(\mathbb{Z}, +)$.

`Solution:` *This imitates the proof that determined all subgroups of the cyclic group C_n. The difference is that we are now considering an infinite cyclic group.*

Let H be a subgroup of $\mathbb{Z}$. $H = \{0\}$ is a possible answer. Otherwise, let $H \neq \{0\}$. Let

$$X = \{d > 0, \ \ d \in H.\}$$

We have $X \neq \emptyset$. Indeed, if $d \in H$ is any nonzero element, then either $d > 0$ or else $-d > 0$ and $-d \in H$ as well. Thus either d or $-d$ are in X, so X is not empty.

Let d be the smallest element of X. We claim that

$$H = d\mathbb{Z} = \{n \in \mathbb{Z} : \ n = dk, \ \ k \in \mathbb{Z}\}.$$

Indeed, since $d \in X$ we have $d \in H$ hence $dk \in H$ for all $k \in \mathbb{Z}$ since H is closed under addition (accounting for $k > 0$) and inverses (to account for $k < 0$). Thus

$$d\mathbb{Z} \subset H.$$

For the opposite inclusion, let $a \in H$ and write

$$a = dk + r$$

where $0 \leq r < d$. We have

$$r = a - dk \in H$$

since $a \in H$ and $-dk \in H$, and H is closed under addition. But if $r > 0$, then $r \in H$ and $0 < r < d$ show $r \in X$, contradicting minimality of d in X. Thus $r = 0$ so $a = dk$. Thus

$$H = d\mathbb{Z}$$

is established by double inclusion.