Midterm Exam Solutions

Math H113, Feb. 25, 2021. Instructor: E. Frenkel

Problem 1.

Consider the group $\mathbb{Z}_{24}$.

(a) Describe its subgroup generated by the element 15.

Since $\text{g.c.d}(24, 15) = 3$, this subgroup is generated by 3 and since $24/3 = 8$, it is isomorphic to $\mathbb{Z}_8$.

(b) Give the list of all elements x of this group with the following property: the cyclic subgroup generated by x is isomorphic to $\mathbb{Z}_4$.

This property is equivalent to $\text{g.c.d}(24, x) = 24/4 = 6$, hence $x \in \{6, 18\}$.

(c) Draw the diagram of all subgroups of $\mathbb{Z}_{24}$.

Here $\langle 1 \rangle = \mathbb{Z}_{24}$ and each arrow denotes an embedding of subgroups:

$$
\begin{array}{ccccccccc}
 & & \langle 1 \rangle & & & & & & \\
 & \nearrow & & \nwarrow & & & & & \\
\langle 3 \rangle & & & & \langle 2 \rangle & & & & \\
 & \nwarrow & & \nearrow & & \nwarrow & & & \\
 & & \langle 6 \rangle & & & & \langle 4 \rangle & & \\
 & & & \nwarrow & & \nearrow & & \nwarrow & \\
 & & & & \langle 12 \rangle & & & & \langle 8 \rangle \\
 & & & & & \nwarrow & & \nearrow & \\
 & & & & & & \langle 0 \rangle & &
\end{array}
$$

Problem 2. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 8 & 4 & 3 & 1 & 2 & 6 \end{pmatrix}$$

(a) Describe the orbits of σ.

$\{1, 7\}, \{2, 5, 4, 8\}, \{3, 9, 6\}$

(b) Express σ as a product of disjoint cycles, and then as a product of transpositions.

$(1, 7)(2, 5, 4, 8)(3, 9, 6) = (1, 7)(2, 8)(2, 4)(2, 5)(3, 6)(3, 9)$

(c) What is the order of σ? Explain.

It is the l.c.m. of the orders of the above cycles, which are 2, 4, and 3. Hence the order of σ is 12.

Problem 3. Let G be a group.

(a) Given two elements $a, b \in G$, define $\phi_{a,b} : \mathbb{Z} \times \mathbb{Z} \to G$ by the formula

$$\phi_{a,b}(m, n) = a^m b^n, \qquad m, n \in \mathbb{Z}.$$

Give the necessary and sufficient conditions on a and b for $\phi_{a,b}$ to be a group homomorphism, and prove that this is so.

The elements $x = (1, 0), y = (0, 1)$ generate $\mathbb{Z}$, and the the relations between are generated by $xy = yx$. Hence any homomorphism $\phi : \mathbb{Z} \to G$ is uniquely determined by a pair of commuting elements $\phi(x)$ and $\phi(y)$ of G. If $\phi = \phi_{a,b}$, these elements are a and b. Hence the necessary and sufficient condition on a and b for $\phi_{a,b}$ to be a group homomorphism is $ab = ba$.

(b) For a positive integer k, define the group $\mathbb{Z}^k$ by induction: $\mathbb{Z}^k = \mathbb{Z} \times \mathbb{Z}^{k-1}$ for $k > 1$, and $\mathbb{Z}^1 = \mathbb{Z}$. Give an explicit description of the set of all homomorphisms $\phi : \mathbb{Z}^k \to G$ in terms of the group G (do not just give the definition) and prove it.

Let x_i be the element of $\mathbb{Z}^k$ whose ith component is 1 and all other components are equal to 0. Then $\mathbb{Z}^k$ is generated by $x_i, i = 1, \dots, k$, and the relations between them are generated by $x_i x_j = x_j x_i$ for all $i \neq j$. Hence any homomorphism $\phi : \mathbb{Z}^k \to G$ is uniquely determined by a k-tuple $a_i = \phi(x_i), i = 1, \dots, k$, of mutually commuting elements of G. Thus, we obtain a one-to-one correspondence between the set of all homomorphisms $\phi : \mathbb{Z}^k \to G$ and the set of such k-tuples.

Problem 4. For each group H below, determine whether the symmetric group S_5 has a subgroup isomorphic to H. If yes, then give an example of such a subgroup. If no, explain why not.

(a) $H = \mathbb{Z}_5$

Yes. $H = \langle (1, 2, 3, 4, 5) \rangle$.

(b) $H = \mathbb{Z}_6$

Yes. $H = \langle (1, 2)(3, 4, 5) \rangle$.

(c) $H = \mathbb{Z}_7$

No. By Lagrange theorem, if $\mathbb{Z}_7$ is a subgroup of G, then 7 must be a divisor of $|G|$. But $|S_5| = 5!$ is not divisible by 7.

Problem 5. Let G be a group.

(a) Suppose that H is a subgroup of G of index 2. Prove that H is a normal subgroup.

Left (resp., right) cosets of H form a partition of G, and one of them is H itself. Since the index of H is equal to 2, we find that there is only one other left (resp., right) coset, which then must be the complement $G \backslash H$. Hence the left cosets coincide with the right cosets, i.e. H is a normal subgroup.

(b) Suppose that H is a subgroup of G of index 3. Either prove that H is a normal subgroup or give a counterexample and explain why it is a counterexample.

Counterexample: $G = S_3, H = \langle(1,2)\rangle$. Then the two elements $(2,3)$ and $(2,3)(1,2)$ are in the same left coset of H, but they are not in the same right coset. Indeed, that would mean that $(1,2)(2,3) = (2,3)(1,2)$ which is not true.

Problem 6. An *automorphism* of a group G is a permutation $f : G \to G$ which is a group isomorphism.

(a) Prove that the set of all automorphisms of a given group G is a subgroup of the group S_G of all permutations of G. Denote it by $\mathrm{Aut}(G)$.

First, we prove that $\mathrm{Aut}(G) \subset S_G$ is closed under the operation of composition: given $f, g \in \mathrm{Aut}(G)$, we find that $f \circ g(ab) = f(g(ab)) = f(g(a)g(b)) = fg(a)fg(b) = (f \circ g)(a)(f \circ g)(b)$.

Second, the identity map $G \to G$ is an isomorphism and hence belongs to $\mathrm{Aut}(G)$.

Third, given $f \in \mathrm{Aut}(G)$, the inverse map f^{-1} is an isomorphism. Indeed, take arbitrary element $a, b \in G$. Since f is an isomorphism, $a = f(a_1), b = f(b_1)$. Hence

$$f^{-1}(ab) = f^{-1}(f(a_1)f(b_1)) = f^{-1}(f(a_1b_1)) = a_1b_1 = f^{-1}(a)f^{-1}f(b).$$

Thus, $f^{-1}(ab) = f^{-1}(a)f^{-1}f(b)$ for all $a, b \in G$.

(b) Describe $\mathrm{Aut}(\mathbb{Z})$.

An isomorphism $\phi : G \to G$ must send a set of generators of G to a set of generators of G (otherwise, ϕ is not surjective). Moreover ϕ is uniquely determined by the image of a particular set of generators.

The group $\mathbb{Z}$ is generated by a single element; namely, 1. Hence an automorphism of $\mathbb{Z}$ must send 1 to a generator of $\mathbb{Z}$. It is clear that none of n with $|n| > 1$ is a generator. This leaves only two possibilities: 1 and -1. Indeed, each generates $\mathbb{Z}$, and they correspond to the identity isomorphism and the sign isomorphism $x \mapsto -x, \forall x \in \mathbb{Z}$, respectively. The composition of the latter isomorphism with itself is the identity. Hence $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}_2$.

(c) Describe $\mathrm{Aut}(\mathbb{Z}_{12})$.

The group $\mathbb{Z}_{12}$ has one generator; namely 1. As stated in (b), an automorphism ϕ of $\mathbb{Z}_{12}$ is uniquely determined by $\phi(1)$ which must be a generator of $\mathbb{Z}_{12}$. Generators of $\mathbb{Z}_{12}$ are its elements s which are relatively prime with 12, i.e. $s \in \{1, 5, 7, 11\}$. Since the relations on s are generated by the relation $12 \cdot s = 0$, each s indeed gives rise to an automorphism ϕ_s of $\mathbb{Z}_{12}$ sending $m \mapsto ms$. Hence we obtain that $\mathrm{Aut}(\mathbb{Z}_{12})$ has 4 elements, so it must be isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein group). To determine which one it is, we take the squares of the homomorphisms ϕ_s. We have $(\phi_s \circ \phi_s)(m) = ms^2$. Since $s^2 = 1 \bmod 12$ for all $s \in \{1, 5, 7, 11\}$, we obtain that $\mathrm{Aut}(\mathbb{Z}_{12}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Problem 7. Describe the group of automorphisms of the symmetric group S_3.

Note: In parts (b) and (c) of Problem 6 and in Problem 7, "describe" means describing the group *and* identifying it with a group we have previously studied.

For any group G, there is a homomorphism $G \to \mathrm{Aut}(G)$ sending $g \in G$ to the inner automorphism ϕ_g of G given by the formula $\phi_g(x) = gxg^{-1}$. However, in general this homomorphism is neither injective nor surjective (for instance, if G is abelian, it sends all $g \in G$ to the identity).

We will prove that the homomorphism $S_3 \to \mathrm{Aut}(S_3)$ is an isomorphism by using the following observation: S_3 has 3 transpositions $\sigma_1 = (1,2), \sigma_2 = (2,3)$, and $\sigma_3 = (1,3)$, and these are the only elements of S_3 of order 2. Now, for any automorphism ϕ of a group G and any $g \in G$, the order of g is equal to the order of $\phi(g)$. Hence every automorphism of S_3 defines a permutation of the set $A = \{\sigma_1, \sigma_2, \sigma_3\}$. Since these transpositions generate S_3, the automorphism itself is unique determined by this permutation.

Thus, we obtain a homomorphism $\mathrm{Aut}(S_3) \to \mathbb{S}_3$ (where $\mathbb{S}_3$ is the group of permutations of $A = \{\sigma_1, \sigma_2, \sigma_3\}$; it is the same group, but I used a different font to distinguish it from the original group S_3 of permutations of the set $\{1,2,3\}$).

Thus, we have constructed homomorphisms $S_3 \to \mathrm{Aut}(S_3)$ and $\mathrm{Aut}(S_3) \to \mathbb{S}_3$. Their composition is a homomorphism $S_3 \to \mathbb{S}_3$. I claim that the latter is an isomorphism, which immediately implies that both $S_3 \to \mathrm{Aut}(S_3)$ and $\mathrm{Aut}(S_3) \to \mathbb{S}_3$ are isomorphisms (indeed, if one of them were not an isomorphism, their composition would not be an isomorphism).

To see that $S_3 \to \mathbb{S}_3$ is an isomorphism, note that $A = \{\sigma_1, \sigma_2, \sigma_3\} = \{(1,2), (2,3), 1,3)\}$ is the set of all unordered pairs of elements of the set $\{1,2,3\}$. Every permutation of $\{1,2,3\}$ gives rise to a permutation of A, and this map is precisely the homomorphism $S_3 \to \mathbb{S}_3$ that we are considering. To see that this is a bijection, consider the complement of each pair: $(1,2) \mapsto 3, (2,3) \mapsto 1, (1,3) \mapsto 2$. It then becomes clear that every permutation of A defines a permutation of $\{1,2,3\}$. Hence we obtain the inverse homomorphism to our homomorphism $S_3 \to \mathbb{S}_3$, so it is indeed an isomorphism.