Test Preparations for Test #2
Math 5310/6310.

Exercises on the isomorphism theorems:

(A) Let $G = (\mathbb{Z}_{200}, +_{200})$, $H = (\mathbb{Z}_{25}, +_{25})$ and $\varphi : G \to H$ be defined by $\varphi([x]_{200}) = [3x]_{25}$. Show that the function is well defined and a homomorphism. Then show how the first isomorphism is witnessed in this situation and prove that the relevant groups are isomorphic and find an isomorphism between them. (I.e. prove $G/\ker(\varphi)$ is isomorphic to H.)

Solution Outline. Since all the groups involved are cyclic groups (this needs to be shown), in order to prove two such groups are isomorphic it is sufficient to prove that they are cyclic and have the same number of element. So work through the following steps:

Step 1. $K = \ker(\varphi) = \{[25n]_{200} | n \in \mathbb{N}\} = \{0, 25, 50, \ldots, 175\}$ so by counting $|K| = 8$.

Step 2. A check of step 1: The element $[25]_{200}$ generates K so $|K| = \frac{200}{25} = 8$.

Step 3. The element $K + [1]_{200}$ generates G/K and so $G/K = \{K, K + [1]_{200}, K + [2]_{200}, \ldots, K + [24]_{200}\}$ and $|G/K| = 25$.

Step 4. Since groups H and G/K are both cyclic groups of size 25, they are isomorphic.

Step 5. Both the following functions are isomorphisms - the second comes from the details of the proof of the first isomorphism theorem.

$$\begin{aligned} \psi_1(K + [n]_{200}) &= [n]_{25} \\ \psi_2(K + [n]_{200}) &= [3n]_{25}. \end{aligned}$$

□

(B) Let $G = (\mathbb{Z}_{1000}, +_{1000})$, $H = \{[20m]_{1000} | m \in \mathbb{N}\}$, $N = \{[25m]_{1000} | m \in \mathbb{N}\}$. Prove that HN/N is isomorphic to $H/(H \cap N)$.

Solution Outline. We use the same strategy as above in A. Since we are using the operation $+_{1000}$, HN means $H +_{1000} N$. Let $+$ denote $+_{1000}$ below.

Step 1. Show that the sizes of H and N are 50 and 40 respectively.

Step 2. Since the greatest common divisor of 20 and 25 is 5; $H + N = \{[5n]_{200} | n \in \mathbb{N}\}$.

Step 3. The element $[5]_{1000}$ generates $H + N = \{0, 5, 10, \ldots, 995\}$ so $|H + N| = \frac{1000}{5} = 200$.

Step 4. The least common multiple of 20 and 25 is 100 so $H \cap N = \{[100m]_{1000}\}$ and so $|H \cap N| = 10$.

Step 5. $(H + N)/N$ is generated by $\{N +_{1000} [5]_{1000}\}$ and is the group $\{N, N + [5]_{1000}, N + [10]_{1000}, \ldots, N + [20]_{1000}\}$. So $|(H + N)/N| = \frac{200}{40} = 5$.

Step 6. $H/H \cap N$ is generated by $H \cap N + [20]_{1000}$ and consists of the elements $\{H \cap N, H \cap N + [20]_{1000}, \ldots, H \cap N + [80]_{1000}\}\}$. So $|H/H \cap N| = \frac{50}{10} = 5$. □

(C) Let $G = (\mathbb{Z}_{1000}, +_{1000})$, $H = \{[20m]_{1000} | m \in \mathbb{N}\}$, $K = \{[200m]_{1000} | m \in N\}$. Prove that G/H is isomorphic to $(G/K)/(H/K)$.

Solution Outline. As above, let $+$ denote $+_{1000}$.

Step 1. Show that the sizes of H and K are 50 and 5 respectively.

Step 2. G/H is generated by $H + [1]_{1000}$ and is the group $\{H, H + [1]_{1000}, H + [2]_{1000}, \ldots, H + [19]_{1000}\}$ and so has 20 elements in it.

Step 3. G/K is generated by $K + [1]_{1000}$ and is the group $\{K, HK + [1]_{1000}, K + [2]_{1000}, \ldots, H + [199]_{1000}\}$ and so has 200 elements in it.

Step 4. H/K is generated by $K + [20]_{1000}$ and is the group $\{K, K + [20]_{1000}, K + [40]_{1000}, \ldots, K + [180]_{1000}\}$ and so has 10 elements in it.

Step 5. $(G/K)/(H/K)$ is generated by $H/K + (K + [1]_{1000})$ and is the group $\{H/K, H/K + (K + [1]_{1000}), H/K + (K + [2]_{1000}), \ldots, H/K + (K + [19]_{1000})\}$ and so has 20 elements in it.

Conclusion: Both G/H and $(G/K)/(H/K)$ are cyclic groups with 20 elements and so are isomorphic.

□

Make sure that you can do exercises from the ExerciseUnit05 notes.

Make sure that you can prove the theorems and do the exercises from the 06 AlgebraNotes

Use the following theorems (referenced earlier in the course and is typically covered in Math 3100) to prove the next couple of theorems. (I will not ask for proofs of these theorems as they are typically covered in another class.):

Theorem I. If n and m are positive integers then d is the greatest common divisor of n and m if and only if there exists integers x and y (which may be negative) so that:

$$d = xn + ym.$$

Theorem II. Suppose that a and b are positive integers; let d be the greatest common divisor of a and b and let m be the least common multiple. Then:

$$ab = dm.$$

Theorem 1. Suppose that G is a cyclic group of order n with generator a. Then a^k generates G if and only if $k = 1$ or n and k are relatively prime.

Exercise 2. Consider $(\mathbb{Z}_{15}, \cdot_1 5)$; let $M_{15} = \{x \in \mathbb{Z}_{15} \mid x \text{ has a multiplicative inverse}\}$. Then list the elements of M_{15} and show that $(M_{15}, \cdot_{15})$ is a group.

Exercise 3. Prove (using induction) that 15 divides $7^{8n} - 1$ for each positive integer n. [Lead-in to the next unit: how did I determine that 15 divided this number?]

Exercise 4. Consider the permutation group S_7.

a. Show that the subgroup generated by the element $(1, 2, 3, 4, 5, 6)$ is a cyclic group of order 6.

b. Show that the subgroup generated by the element $(1, 3, 4, 5, 6, 7)$ is a cyclic group of order 6.

c. Show that the subgroup generated by the element $(1, 2, 3)$ is a cyclic group of order 3.

d. Show that the subgroup generated by the element $(6, 7)$ is a cyclic group of order 2.

e. Show that the permutations $(1, 2, 3)$ and $(6, 7)$ commute and generates a cyclic group of order 6.

f. Show that the $(1, 2)$ and $(6, 7)$ commute and generates a non-cyclic group of order 4.