MATH 415

Modern Algebra I

Lecture 19:
Review for Exam 1.

Topics for Exam 1

Group theory:

- Binary operations
- Groups
- Subgroups, cyclic groups
- Groups of permutations
- Cosets, Lagrange's theorem
- Direct product of groups
- Factor groups
- Homomorphisms of groups
- Classification of abelian groups
- Group actions

Fraleigh/Brand: Sections 0–14

Sample problems

Problem 1. Consider an operation $*$ defined on the set $\mathbb{Z}$ of integers by $a * b = a + b - 2$. Does this operation provide the integers with a group structure?

Problem 2. Suppose $(S, *)$ is a semigroup satisfying the following two conditions:
(i) there exists $e \in S$ such that $e * g = g$ for all $g \in S$ (**existence of a left identity element**);
(ii) for any $g \in S$ there exists $g' \in S$ such that $g' * g = e$ (**existence of a left inverse**).
Prove that $(S, *)$ is a group.

Sample problems

Problem 3. Prove that the group $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not cyclic.

Problem 4. Let G be a group of order 125. Show that G contains an element of order 5.

Problem 5. Find the order and the sign of the permutation $\sigma = (1\ 2)(3\ 4\ 5\ 6)(1\ 2\ 3\ 4)(5\ 6)$.

Problem 6. Suppose $\pi, \sigma \in S_5$ are permutations of order 3. What are possible values for the order of the permutation $\pi\sigma$?

Sample problems

Problem 7. Find all subgroups of the alternating group A_4.

Problem 8. Determine which of the following groups of order 12 are isomorphic and which are not: $\mathbb{Z}_{12}$, $\mathbb{Z}_3 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, $S_3 \times \mathbb{Z}_2$, A_4 and D_6.

Problem 9. Find an example of an abelian group G and its subgroups H_1 and H_2 such that the subgroups H_1 and H_2 are isomorphic while the factor groups G/H_1 and G/H_2 are not.

Sample problems

Problem 10. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A			
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

Problem 1. Consider the operation $*$ defined on the set $\mathbb{Z}$ of integers by $a * b = a + b - 2$. Does this operation provide the integers with a group structure?

First we check that the operation $*$ is well defined:
$a, b \in \mathbb{Z} \implies a * b = a + b - 2 \in \mathbb{Z}$.

Then we need to check 3 axioms.

Associativity: for any $a, b, c \in \mathbb{Z}$, we have
$(a*b)*c = (a+b-2)*c = (a+b-2)+c-2 = a+b+c-4$,
$a*(b*c) = a*(b+c-2) = a+(b+c-2)-2 = a+b+c-4$,
hence $(a * b) * c = a * (b * c)$.

Existence of identity: equations $a * e = e * a = a$ are equivalent to $e + a - 2 = a$. They hold for $e = 2$.

Existence of inverse: equations $a * b = b * a = e$ are equivalent to $b + a - 2 = e$ $(= 2)$. They hold for $b = 4 - a$.

Thus $(\mathbb{Z}, *)$ is a group.

Problem 1. Consider the operation $*$ defined on the set $\mathbb{Z}$ of integers by $a * b = a + b - 2$. Does this operation provide the integers with a group structure?

Alternative solution: First we check that the operation $*$ is well defined: $a, b \in \mathbb{Z} \implies a * b = a + b - 2 \in \mathbb{Z}$.

Then we observe that $a * b - 2 = (a - 2) + (b - 2)$ for all $a, b \in \mathbb{Z}$. Consider a function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(a) = a - 2$. We obtain that $f(a * b) = f(a) + f(b)$ for all $a, b \in \mathbb{Z}$. This means that f is a homomorphism of the binary structure $(\mathbb{Z}, *)$ to the binary structure $(\mathbb{Z}, +)$. It is easy to see that f is bijective. Therefore f is an isomorphism of binary structures. Since all axioms of a group are structural properties (and hence preserved by isomorphisms), it follows that $(\mathbb{Z}, *)$ is a group and that it is isomorphic to the group $(\mathbb{Z}, +)$.

Problem 2. Suppose $(S, *)$ is a semigroup satisfying the following two conditions:
(i) there exists $e \in S$ such that $e * g = g$ for all $g \in S$ (**existence of a left identity element**);
(ii) for any $g \in S$ there exists $g' \in S$ such that $g' * g = e$ (**existence of a left inverse**).

Prove that $(S, *)$ is a group.

Given an element $g \in G$, let g' be a left inverse of g. Further, let g'' be a left inverse of g'. We are going to simplify an expression $g'' * g' * g * g'$ in two different ways:

$$(g'' * g') * (g * g') = e * (g * g') = g * g',$$
$$g'' * ((g' * g) * g') = g'' * (e * g') = g'' * g' = e.$$

By associativity of the operation, $g * g' = e$. Furthermore, $g * e = g * (g' * g) = (g * g') * g = e * g = g$. Thus e is a true (two-sided) identity element and g' is a true (two-sided) inverse of g.

Problem 3. Prove that the group $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not cyclic.

Take any non-zero rational number r. It can be represented as a reduced fraction: $r = \dfrac{m}{n}$, where m and n are non-zero integers and $\gcd(m, n) = 1$.

The cyclic group $\langle r \rangle$ consists of fractions $\dfrac{m}{n}, \dfrac{m^2}{n^2}, \dfrac{m^3}{n^3}, \ldots,$ fractions $\dfrac{n}{m}, \dfrac{n^2}{m^2}, \dfrac{n^3}{m^3}, \ldots,$ and 1. Note that all fractions are reduced.

The numbers m and n can have only finitely many prime divisors. Since there are infinitely many prime numbers, we can find a prime number p that divides neither m nor n. It is easy to see that $p \notin \langle r \rangle$. Thus $\langle r \rangle \neq \mathbb{Q} \setminus \{0\}$.

Problem 4. Suppose G is a group of order 125. Show that G contains an element of order 5.

It follows from Lagrange's Theorem that the order of any element of the group G divides 125. Hence the only orders we can expect are 1, 5, 25, and 125.

Let g be any element of G different from the identity element. Then the order of g is 5, 25 or 125.

If $o(g) = 5$ then we are done.

If $o(g) = 25$ then the element g^5 has order 5.

If $o(g) = 125$ then the element g^{25} has order 5.

Remark. In general, if the order of g is n, then the order of g^k is $\dfrac{n}{\gcd(k, n)}$.

Problem 5. Find the order and the sign of the permutation $\sigma = (1\ 2)(3\ 4\ 5\ 6)(1\ 2\ 3\ 4)(5\ 6)$.

First we need to rewrite the permutation σ as a product of disjoint cycles (this is not necessary to determine the sign, but necessary to determine the order). Keeping in mind that the composition is evaluated from right to left, we find that $\sigma(1) = 1$, $\sigma(2) = 4$, and $\sigma(4) = 2$. Further, $\sigma(3) = 5$ and $\sigma(5) = 3$. Finally, $\sigma(6) = 6$. Thus

$$\sigma = (2\ 4)(3\ 5).$$

It follows that the order of σ is 2 (least common multiple of lengths of the disjoint cycles). Besides, σ is an even permutation so that the sign of σ is $+1$.

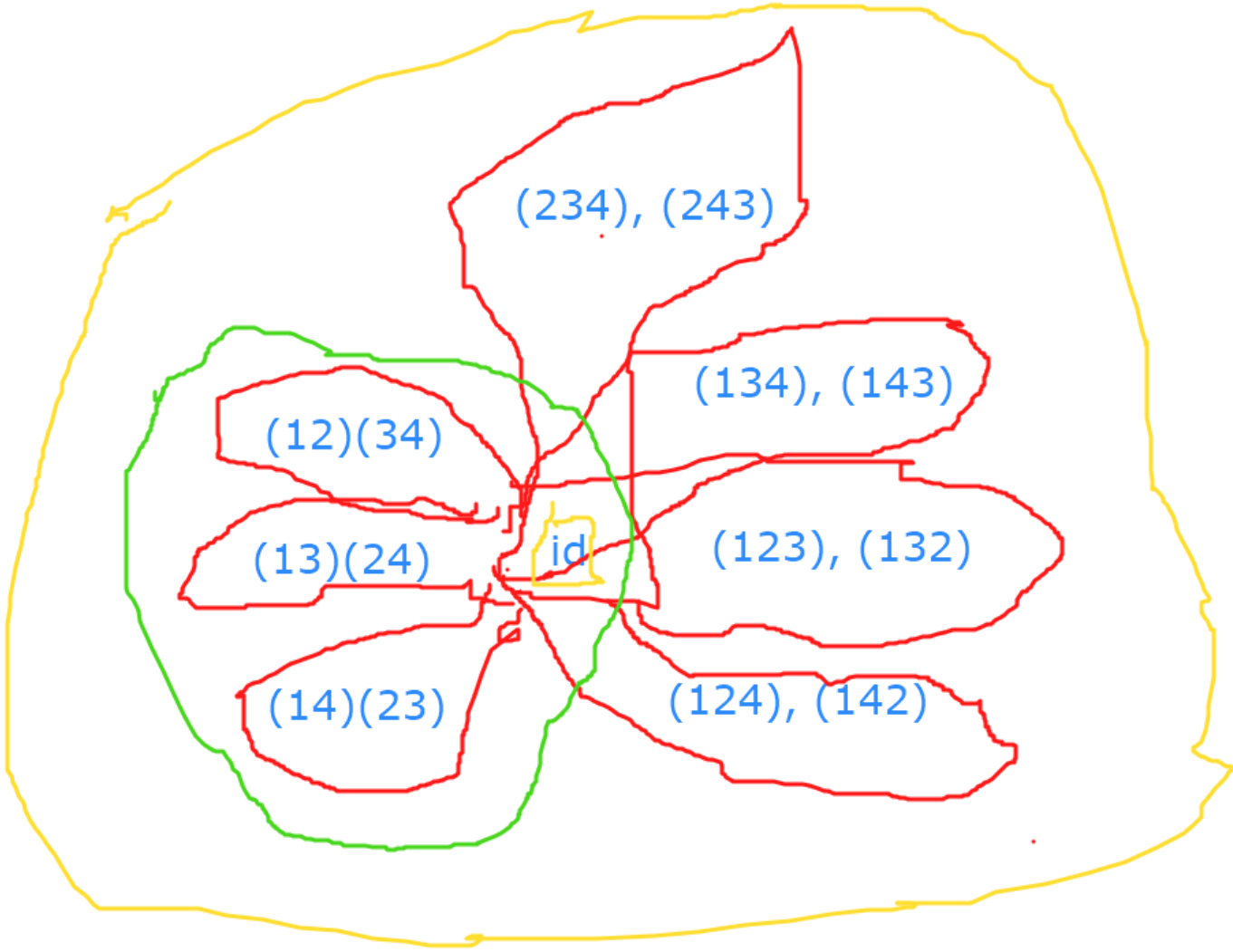
Problem 6. Suppose $\pi, \sigma \in S_5$ are permutations of order 3. What are possible values for the order of permutation $\pi\sigma$.

The order of a permutation equals the least common multiple of the cycle lengths in its cycle decomposition. Hence it equals 3 only if the cycles are of length 1 or 3 (at least one cycle of length 3 is required). For permutations $\pi, \sigma \in S_5$, this implies that both are cycles of length 3.

Up to relabeling of the set $\{1, 2, 3, 4, 5\}$, we can assume that $\pi = (1\ 2\ 3)$. As for σ, there are several possible choices: $\sigma_1 = (1\ 4\ 5)$, $\sigma_2 = (1\ 2\ 4)$, $\sigma_3 = (2\ 1\ 4)$, $\sigma_4 = (1\ 2\ 3)$, and $\sigma_5 = (1\ 3\ 2)$. Namely, $\sigma = \sigma_1$ if there is only one element that both π and σ move, $\sigma = \sigma_2$ or σ_3 if there are two such elements, and $\sigma = \sigma_4$ or σ_5 if π and σ move the same three elements.

We have $\pi\sigma_1 = (1\,4\,5\,2\,3)$, $\pi\sigma_2 = (1\,3)(2\,4)$, $\pi\sigma_3 = (1\,4\,3)$, $\pi\sigma_4 = (1\,3\,2)$, and $\pi\sigma_5 = \mathrm{id}$. Thus the order of $\pi\sigma$ can be 1, 2, 3 or 5.

Problem 7. Find all subgroups of the alternating group A_4.



Problem 8. Determine which of the following groups of order 12 are isomorphic and which are not: $\mathbb{Z}_{12}$, $\mathbb{Z}_3 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, $S_3 \times \mathbb{Z}_2$, A_4 and D_6.

Answer: $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$ and $S_3 \times \mathbb{Z}_2 \cong D_6$ are the only isomorphisms.

The element $(1, 1)$ of the group $\mathbb{Z}_3 \times \mathbb{Z}_4$ has order 12. Therefore it generates the entire group so that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is cyclic. Hence this group is isomorphic to $\mathbb{Z}_{12}$ as another cyclic group of order 12. On the other hand, the group $\mathbb{Z}_2 \times \mathbb{Z}_6$ has no element of order 12.

The first three of the given groups are abelian while the last three are not. Hence there is no isomorphism between the first three and the last three.

The groups $S_3 \times \mathbb{Z}_2$ and D_6 have elements of order 6 while the group A_4 has none. Therefore A_4 is not isomorphic to $S_3 \times \mathbb{Z}_2$ or D_6. The isomorphism $S_3 \times \mathbb{Z}_2 \cong D_6$ was established in the previous lecture.

Problem 9. Find an example of an abelian group G and its subgroups H_1 and H_2 such that the subgroups H_1 and H_2 are isomorphic while the factor groups G/H_1 and G/H_2 are not.

Let $G = \mathbb{Z}$, $H_1 = 2\mathbb{Z}$ and $H_2 = 3\mathbb{Z}$. Then G, H_1 and H_2 are infinite cyclic groups. Hence they are all isomorphic. On the other hand, $G/H_1 \cong \mathbb{Z}_2$ and $G/H_2 \cong \mathbb{Z}_3$ are groups of different order.

If G is a finite abelian group and H_1 and H_2 are isomorphic subgroups, then both subgroups have the same order and the same index. Therefore the factor groups G/H_1 and G/H_2 are of the same order. But they need not be isomorphic.

Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, $H_1 = \{0\} \times \mathbb{Z}_2$ and $H_2 = \{0, 2\} \times \{0\}$. Then H_1 and H_2 are cyclic groups of order 2. On the other hand, $G/H_1 \cong \mathbb{Z}_4$, a cyclic group, while $G/H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, a non-cyclic group.

Problem 10. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A		B	
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

First we observe that E is the identity element as $E^2 = E$. Next we observe that $A^2 = I$ and $A^3 = AI = F$ so that the order of A is greater than 3. Since the order of the group is 9, it follows from Lagrange's theorem that A has order 9. Therefore the group is cyclic and A is a generator. Further, $B = F^2 = A^6$, $C = I^2 = A^4$, $H = C^2 = A^8$, $D = H^2 = A^{16} = A^7$, $G = D^2 = A^{14} = A^5$. Also, $E = A^0$. Now that every element of the group is represented as a power of A, completing the table is a routine task. For example, $DH = A^7A^8 = A^{15} = A^6 = B$.