MATH 100: Homework #3

Due on October 19, 2023 at 12:00pm

Professor McKernan

Section A02 5:00PM - 5:50PM
Section Leader: Castellano

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai
A16848188

Problem 1

"The union of two subgroups of a group G is a subgroup of G." True or False? If true then give a proof and if false then give a counterexample.

Proof. The statement is false. Consider the D_3, the groups of symmetries of a triangle, and its subgroups $\{I, F_1\}$, $\{I, F_2\}$, two cyclic subgroups of distinct flips. Since $F_1 F_2 = R$, their union $\{I, F_1, F_2\}$ is not closed under the operation of G, and thus it's not a subgroup. $\square$

Problem 2

Verify that the relation $\sim$ is an equivalence relation on the set S given.

(b) $S = \mathbb{C}$, the complex numbers, $a \sim b$ if $|a| = |b|$.

Proof. We check each property of a equivalence relation.

Reflexivity: $|a| = |a|$, and so $a \sim a$, trivial.

Symmetry: Suppose that $|a| = |b|$, then $|b| = |a|$. Thus, $a \sim b$ imples $b \sim a$.

Transitivity: Suppose that $a \sim b$ and $b \sim c$. Then $|a| = |b| = |c|$, and so $a \sim c$.

Thus, $\sim$ is an equivalence relation. Its equivalence classes are sets of complex numbers of the same distance to the origin, namely, circles of different radius centering the origin on the complex plane. $\square$

(c) $S =$ straight lines in the plane, $a \sim b$ if a, b are parallel.

Proof. We again check each property of a equivalence relation.

Reflexivity: a is paralled to itself so $a \sim a$.

Symmetry: Suppose that $a \sim b$. Then a, b are parallel to each other, and so $b \sim a$.

Transitivity: Suppose that $a \sim b$ and $b \sim c$. Let s be the slope of b. Since $a \sim b$ and $b \sim c$, the slope of a, b, c are all s, and so $a \sim c$.

Thus, $\sim$ is an equivalence relation. Its equivalence classes are sets of straight lines with the same slope. $\square$

Problem 3

For each subgroup of D_4, list all the left and right cosets. (Since D_4 has many subgroups, it is only necessary to do this up to the obvious symmetries)

Proof. The left and right cosets of $\{I\}$ are all the sets that only contain a non-identity element in D_4.

The left and right cosets of D_4 is D_4 itself.

Since $\{I, R_1, R_2, R_3\}$ contains 4 elements, by the Lagrange Theorem, the only possible left/right cosets of it is $\{I, R_1, R_2, R_3\}$ itself and the rest of the elements $\{F_1, F_2, F_3, F_3\}$, namely, all of the flips.

For $\{I, F_1\}$, its left cosets are $\{I, F_1\}, \{F_2, R^2\}, \{F_3, R\}, \{F_4, R^3\}$, while while the right cosets are $\{I, F_1\}, \{F_2, R^2\}, \{F_3, R^3\}, \{F_4, R\}$.

For $\{I, F_2\}$, its left cosets are $\{I, F_2\}, \{F_1, R^2\}, \{F_3, R^3\}, \{F_4, R\}$, while while the right cosets are $\{I, F_2\}, \{F_1, R^2\}, \{F_3, R\}, \{F_4, R^3\}$.

For $\{I, F_3\}$, its left cosets are $\{I, F_3\}, \{F_1, R^3\}, \{F_2, R\}, \{F_4, R^2\}$, while while the right cosets are $\{I, F_3\}, \{F_1 R\}, \{F_2, R^3\}, \{F_4, R^2\}$.

For $\{I, F_4\}$, its left cosets are $\{I, F_4\}, \{F_1, R\}, \{F_2, R^3\}, \{F_4, R^2\}$, while while the right cosets are $\{I, F_4\}, \{F_1 R^3\}, \{F_2, R\}, \{F_4, R^2\}$.

For $\{I, R^2\}$, its left and right cosets are both $\{I, R^2\}, \{R, R^3\}, \{F_1, F_2\}, \{F_3, F_4\}$. $\square$

Problem 4

In $\mathbb{Z}_{16}$, write down all the cosets of the subgroup $H = \{[0], [4], [8], [12]\}$.

Proof.

$$\begin{aligned}
[0] + H &= H \\
[1] + H &= \{[1], [5], [9], [13]\} \\
[2] + H &= \{[2], [6], [10], [14]\} \\
[3] + H &= \{[3], [7], [11], [15]\}
\end{aligned}$$

Since $[4] + H = [0] + H = H$, $[a] + H$ repeats the above listed cosets, for all $a \geq 4$.

Thus, we have obtained all cosets of H. $\square$

Problem 5

In problem 4, what is the index of H in $\mathbb{Z}_{16}$?

Proof. As listed in above question, there are 4 left/right cosets of H, and thus $[\mathbb{Z}_{16}; H] = 4$. $\square$

Problem 6

If aH and bH are distinct left cosets of H in G, are Ha and Hb distinct right cosets of H in G?

Proof. No. Consider D_4's subgroup $H = \{I, F_1\}$. From problem 3, we know $F_3H = \{F_3, R\}$ and $R^3H = \{F_4, R_3\}$ are distinct cosets. However $HF_3 = \{F_3, R^3\} = HR^3$ are the same. Thus the statement is disproved. $\square$

Problem 7

If G is a finite abelian group and $a_1, \dots, a_n$ are all elements, show that $x = a_1 a_2 \dots a_n$ must satisfy $x^2 = e$.

Proof. We first prove that for all $k \geq 1$, $\Pi_{1 \leq j \leq k} a_j = a_k \Pi_{1 \leq j < k} a_j$. Let $y = \Pi_{1 \leq j \leq k} a_j \in G$. Since G is abelian,

$$\Pi_{1 \leq j \leq k} a_j = y a_k = a_k y = a_k \Pi_{1 \leq j < k} a_j. \tag{1}$$

We now prove that we can rearrange $x = a_1 a_2 \dots a_n$ into any ordering by induction on n. The base case is trivial. For $n > 1$, suppose we aim to rearrange $x = a_1 a_2 \dots a_n$ into some ordering such that a_n is the l-th element in the order. We can first take the last $n - l + 1$ elements and apply (1) to move a_n to the l-th position. Then, by induction, we can rearrange the first $l - 1$ elements and the last $n - l$ elements into the desired ordering, and thus the statement is proven.

Since each element has one unique inverse, we can rearrange $x = a_1 a_2 \dots a_n$ into $x = a_{m_n} a_{m_{n-1}} \dots a_{m_1}$, such that $a_i a_{m_i} = e$ for all $1 \leq i \leq n$. Therefore,

$$\begin{aligned} x^2 &= a_1 a_2 \dots a_{n-1} (a_n a_{m_n}) a_{m_{n-1}} \dots a_{m_1} \\ &= a_1 a_2 \dots a_{n-2} (a_{n-1} a_{m_{n-1}}) a_{m_{n-2}} \dots a_{m_1} \\ &= a_1 a_{m_1} \\ &= e. \end{aligned}$$

$\square$

Problem 8

If G is of odd order, what can you say about the x in problem 16?

Proof. Since G is of odd order, G cannot have subgroups of order 2, and thus for all non indentity $a \in G$, $a^2 \neq e$, otherwise $\{e, a\}$ would a a subgroup of order 2 in G. This implies that each non-identity element can be paired with an unique inverse distinct to itself. By the result we obtained in the previous question, we can rearrange x such that each non-identity element in the sequence is next to its inverse. By associativity, each non-identity element in the new ordering would pair up with its neighboring inverse and resolve to e, and thus we get $x = e$. $\square$

Problem 9

Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a 1-1 mapping of S onto T.

Proof. Consider the function $f : S \to T$, $f(Hx) = x^{-1}H$, for $x \in G$. Let $Ha, Ha' \in S$, such that $Ha = Ha'$. This implies that $Haa'^{-1} = H$, and so $aa'^{-1} \in H$. Let $h = aa'^{-1}$. We know $a^{-1}h = a^{-1}aa'^{-1} = a'^{-1} \in a^{-1}H$, and thus $f(Ha) = a^{-1}H = a'^{-1}H = f(Ha')$.

We first show f is injective. Let $a, b \in G$, such that $f(Ha) = f(Hb)$. Then, we know $a^{-1}H = b^{-1}H$, and so $ba^{-1}H = H$, which implies $ba^{-1} \in H$. Let $h = ba^{-1} \in H$. We then get $ha = b \in Ha$, and thus $Ha = Hb$.

We now show f is surjective. For all $y = bH \in T$, we have $x = Hb^{-1} \in S$, so that $f(x) = bH$.

Therefore, f is a 1-1 mapping of S onto T. □

Problem 10

If $aH = bH$ forces $Ha = Hb$ in G, show that $aHa^{-1} = H$ for every $a \in G$.

Proof. Let $b \in aH$. Then, $aH = bH$, which forces $b \in Hb = Ha$. Thus, $aH \subseteq Ha$, so $aHa^{-1} \subseteq H$. We now show that $|aHa^{-1}| \geq |H|$. Define $f : aHa^{-1} \to H$ as $f(x) = a^{-1}xa$.

Let $x = aha^{-1}, x' = ah'a^{-1}$, for some h, h', such that $x = x'$. By cancellation, we know $h = h'$. Then, $f(x) = a^{-1}xa = h = h' = a^{-1}x'a = f(x')$, and so f is well defined.

For each $y \in H$, we have $x = aya^{-1}$, such that $f(x) = a^{-1}(aya^{-1})a = y$. Thus, f is surjective, and so $|aHa^{-1}| \geq |H|$. Since $aHa^{-1} \subseteq H$ and $|aHa^{-1}| \geq |H|$, we have $aHa^{-1} = H$. $\square$

Problem 11

If in a group G, $aba^{-1} = b^i$, show that $a^r ba^{-r} = b^{i^r}$ for all positive integers r.

Proof. We proceed by induction on r. The base case $aba^{-1} = b^i$ is already given. For $r > 1$, we get $a^r ba^{-r} = a \cdot a^{r-1}ba^{-(r-1)} \cdot a^{-1}$. By induction,

$$\begin{aligned} a \cdot a^{r-1}ba^{-(r-1)} \cdot a^{-1} &= ab^{i^{r-1}}a^{-1} \\ &= \underbrace{aba^{-1}aba^{-1}\dots aba^{-1}}_{i^{r-1} \text{ times}} \\ &= (b^i)^{i^{r-1}} \\ &= b^{i^r}, \end{aligned}$$

and we are done. $\square$

Problem 12

If in G, $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$.

Proof. Since $aba^{-1} = b^2$, by the result we obtained from the previous question, we know $a^5ba^{-5} = b = b^{2^5}$, and thus we get $b^{2^5-1} = e$. Since $2^5 - 1 = 31$ is a prime number and $b \neq e$, there are no positive $r < 31$ such that $b^r = e$, and so $o(b) = 31$. $\square$

Challenge Problems

Problem 13

Let G be an abelian group of order n, and $a_1, \dots, a_n$ its elements. Let $x = a_1 a_2 \dots a_n$. Show that:

(a) If G has exactly one element $b \neq e$ such that $b^2 = e$, then $x = b$.

Proof. In problem 7, we proved that we can rearrange $x = a_1 a_2 \dots a_n$ into any ordering. For all $a_i^2 \neq e$, we rearrange $a_1 a_2 \dots a_n$ such that a_i is next it its inverse, which allows each a_i to pair up with its neighboring inverse and resolve to e. Thus, the sequence becomes $x = be = e$, and we are done. □

(b) If G has more than one element $b \neq e$ such that $b^2 = e$, then $x = e$.

Proof. idk bro. □

(c) If n is odd, then $x = e$.

Proof. Proved in problem 8. □

Problem 14

"Every countable group is finitely generated." True or False? If true then give a proof and if false then give a counterexample.

Proof. Consider $\mathbb{Q}$ under addition. We know $\mathbb{Q}$ is countable. Suppose for sake of contradiction that there exists a finite set $S = \{s_1, s_2, \ldots, s_n\} \subset \mathbb{Q}$, $s_i = \frac{a_i}{b_i}$ for $a_i, b_i \in \mathbb{Z} - \{0\}$, such that $\langle S \rangle = \mathbb{Q}$. Let $b = \Pi_{s_i \in S} b_i$. Then, all elements in $\langle S \rangle$ can be represented in the form of $\frac{c_i}{b}$, $c_i \in \mathbb{Z}$. However, we can find $\frac{p}{q} \in \mathbb{Q}$, such that $p, q \in \mathbb{N}$, $\gcd(q, b) = 1$, so that $\frac{p}{q}$ cannot be represented in the form of $\frac{c_i}{b}$, contradiction. Therefore, $\mathbb{Q}$ under addition is a countable group that cannot be finitely generated. $\square$