Nathan Bickel
MATH 546: Section
Professor: Dr. Vraciu
October 9, 2023

MATH 546 Homework 5

Problem 1 List all the elements of the group $\mathbb{Z}_{15}^*$. Decide whether it is a cyclic group or not. If it is cyclic, find a generator. Justify your answer.

Solution.

We have

$$\mathbb{Z}_{15}^* = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}.$$

If G is a cyclic group, then there exists some $a \in G$ such that $\langle a \rangle = G$, which we have shown implies $o(a) = |G|$. However, through exponentiation it can be verified that

$$o([1]_{15}) \leq 1, o([2]_{15}) \leq 4, o([4]_{15}) \leq 2, o([7]_{15}) \leq 4, o([8]_{15}) \leq 4, o([11]_{15}) \leq 2, o([13]_{15}) \leq 4, o([14]_{15}) \leq 2.$$

Since all of the orders are less than $|\mathbb{Z}_{15}^*| = 8$, $\mathbb{Z}_{15}^*$ is not cyclic. $\square$

Problem 2 Let G be a group with $|G| = 8$. Assume that a, b are elements of G and $ab \neq ba$. Also assume that H is a subgroup of G, and $a, b \in H$. Prove that H must be equal to the entire G.

Solution.

By Lagrange's Theorem, we must have $|H|$ divides $|G|$. The factors of 8 are 1, 2, 4, and 8, so $|H|$ must take on one of these values. Suppose toward contradiction that $|G| \neq |H|$.

- Case 1: $|H| = 1$. But then $a = b$ is the only element, contradicting $ab \neq ba$.
- Case 2: $|H| = 2$. Since H is a subgroup, it has an identity e, so $a = e$ or $b = e$. But this contradicts $ab \neq ba$, because left-multiplication and right-multiplication by the identity yield the same result.
- Case 3: $|H| = 4$. Since H is a subgroup, it has an identity e, and as shown above, we must have that a and b are distinct elements not equal to the identity. So these are three of the elements in H, and we must have a fourth distinct element $c \in H$ from G.

  Consider ab and ba, which are in H by closure. We cannot have $ab = e$ or $ba = e$, because then $a = b^{-1}$ and we would have $ab = e = ba$. We also cannot have $ab = a$, $ab = b$, $ba = a$, or $ba = b$, because appropriate multiplying by an inverse shows that one of the elements is the identity, a contradiction as shown in Case 2. So the only possibility is $ab = c = ba$, a contradiction since $ab \neq ba$.

So the only possibility is that $|H| = |G|$, and since $H \subseteq G$, we must have $H = G$. $\square$

Problem 3 Let G be a group with $|G| = 6$. Assume that the elements of G are e, a, b, a^2, ab, a^2b, where e is the identity and all 6 elements listed are assumed to be distinct. Further assume that $a^3 = e$, $b^2 = e$, and $ba = a^2b$. Find all the subgroups of G. For each subgroup describe it by listing each element. Explain why all the subgroups you are listing are indeed subgroups. Also explain why there are no other subgroups.

Solution.

We will first find the star table of G. By repeated application of the information given, we will obtain:

$*$	e	a	b	a^2	ab	a^2b
e	e	a	b	a^2	ab	a^2b
a	a	a^2	ab	e	a^2b	b
b	b	a^2b	e	ab	a^2	a
a^2	a^2	e	a^2b	a	b	ab
ab	ab	b	a	a^2b	e	a^2
a^2b	a^2b	ab	a^2	b	a	e

By Lagrange's theorem, any subgroup H will have $|H|$ divides $|G|$. The factors of 6 are $1, 2, 3, 6$, so any H will take on one of these values.

If $|H| = 1$ or $|H| = 6$, then $H = \{e\}$ or $H = G$ respectively. These are both known to be subgroups. If $|H| = 2$, then we must have $H = \{e, x\}$ for some $x \neq e$, and where $x^2 = e$ (we cannot have $x^2 = x$ or $x = e$, and otherwise x^2 would be in the subgroup). Then, x is its own inverse and so is e, so H is a subgroup of size 2 if and only if this holds. If $|H| = 3$, we must have $e \in H$, so we will have two other distinct elements from G. So there are $\binom{5}{2}$ subsets to check. We now list the subgroups with justification:

1. $\{e\}$: Known.
2. $\{e, b\}$: Satisfies above characterization because $b^2 = e$.
3. $\{e, ab\}$: Satisfies above characterization because $(ab)^2 = e$.
4. $\{e, a^2b\}$: Satisfies above characterization because $(a^2b)^2 = e$.
5. $\{e, a, a^2\}$: Equals $< a >$, which is known to be a subgroup.
6. $\{e, a, b, a^2, ab, a^2b\}$: Known.

Any subgroup of size 4 or 5 will not work because of Lagrange, and all subgroups of size 2 not listed do not satisfy the characterization. For the other subgroups of size 3 with the identity, they are not subgroups because closure fails:

- $\{e, a, b\}$: $aa = a^2 \notin H$.
- $\{e, a, ab\}$: $aa = a^2 \notin H$.
- $\{e, a, a^2b\}$: $aa = a^2 \notin H$.
- $\{e, b, a^2\}$: $a^2a^2 = a \notin H$.
- $\{e, b, ab\}$: $bab = a^2 \notin H$.
- $\{e, b, a^2b\}$: $ba^2b = a \notin H$.
- $\{e, a^2, ab\}$: $a^2a^2 = a \notin H$.
- $\{e, a^2, a^2b\}$: $a^2a^2 = a \notin H$.

- $\{e, ab, a^2b\}$: $aba^2 = a^2 \notin H$.

So the subgroups listed are the only ones possible. $\square$

Problem 4 Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(a) What are the possible orders of the subgroups of G? Explain.

(b) Give 4 different examples of subgroups of G of order 2.

(c) Give 4 different examples of subgroups of G of order 4.

Solution.

(a) We have shown in class that $|A \times B| = |A||B|$, so $|\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2| = |2||2||2| = 8$. By Lagrange's theorem, any subgroup H has $|H| \mid |G|$, and since the factors of 8 are $1, 2, 4, 8$, any subgroup will have order in $\{1, 2, 4, 8\}$. Further, it will contain the identity $e = ([0]_2, [0]_2, [0]_2)$.

(b) We can use that $[1]_2 + [1]_2 = [0]_2$ to say that

$$\{e, ([1]_2, [0]_2, [0]_2)\}, \{e, ([0]_2, [1]_2, [0]_2)\}, \{e, ([0]_2, [0]_2, [1]_2)\}, \{e, ([1]_2, [1]_2, [1]_2)\}$$

are all subgroups: the non-identity elements are all their own additive inverses, so adding them yields the identity and thus closure holds.

(c) We can use similar reasoning to show that the following are subgroups:

- $\{([0]_2, [0]_2, [0]_2), ([1]_2, [0]_2, [0]_2), ([0]_2, [1]_2, [0]_2), ([1]_2, [1]_2, [0]_2)\}$,
- $\{([0]_2, [0]_2, [0]_2), ([1]_2, [0]_2, [0]_2), ([0]_2, [0]_2, [1]_2), ([1]_2, [0]_2, [1]_2)\}$,
- $\{([0]_2, [0]_2, [0]_2), ([0]_2, [1]_2, [0]_2), ([0]_2, [0]_2, [1]_2), ([0]_2, [1]_2, [1]_2)\}$,
- $\{([0]_2, [0]_2, [0]_2), ([1]_2, [1]_2, [0]_2), ([1]_2, [0]_2, [1]_2), ([0]_2, [1]_2, [1]_2)\}$.

Problem 5 Let $G = \mathbb{Z}_{240}$, $a = [9]_{240}$, $b = [25]_{240}$. Assume that H is a subgroup of G and $a, b \in H$. Prove that H must be equal to the entire G.

By closure, we must have

$$4 \cdot [25]_{240} + (-11) \cdot [9]_{240} = [100]_{240} + [-99]_{240} = [1]_{240} \in H.$$

But then we certainly have $H = G$, since $x \in G$ satisfies $x = x \cdot [1]_{240} \in H$ by closure. $\square$

Problem 6

(a) For $G = \mathbb{Z}_{15}$, give an example of two subgroups H and K that are both not equal to $\{[0]_{15}\}$, but $H \cap K = \{[0]_{15}\}$.

(b) For $G = \mathbb{Z}$, prove that if H and K are subgroups that are both not equal to $\{0\}$, then $H \cap K \neq \{0\}$.

Solution.

(a) Consider

$$H = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}, K = \{[0]_{15}, [5]_{15}, [10]_{15}\}.$$

We have shown in class that groups of this form are subgroups under addition, and $H \cap K = \{[0]_{15}\}$.

(b) We have showed in class that any subgroup of $\mathbb{Z}$ has the form $k\mathbb{Z}$ for some $k \in \mathbb{Z}$. Since $H \neq \{0\} \neq K$, there exist $h, k \in \mathbb{Z}\backslash\{0\}$ such that $H = h\mathbb{Z}$, $K = k\mathbb{Z}$. But then $hk \in H$ since $k \in \mathbb{Z}$ and $hk \in K$ since $h \in \mathbb{Z}$, so $hk \in H \cap K$. Since $h \neq 0 \neq k$, we have $hk \neq 0$. Therefore, $H \cap K \neq \{0\}$.

$\square$