Modern Algebra 1

Grant Talbert
09/26/24
Dr. Duque-Rosero
MA 541 Section A1

Boston University

Problem 1

Solution. For convenience, let I always denote the 2×2 identity matrix within this problem, and let $H \coloneqq \left\{\alpha I \mid \alpha \in \mathbb{Z}_n \wedge \alpha^2 \not\equiv 0 \pmod{n}\right\}$.

First, we show that $H \subseteq Z(\mathrm{GL}_2(\mathbb{Z}_n))$. Let $A \in \mathrm{GL}_2(\mathbb{Z}_n)$, and let $\alpha \in \mathbb{Z}_n$. It follows that

$$(\alpha I)A = \alpha(IA) = \alpha A = A\alpha = (AI)\alpha = A(I\alpha) = A(\alpha I).$$

Thus, for all $A \in \mathrm{GL}_2(\mathbb{Z}_n)$, $\alpha IA = A\alpha I$. Therefore, $H \subseteq Z(\mathrm{GL}_2(\mathbb{Z}_n))$.

Before we show the converse, I have some commentary on the problem. The first line of the problem states $\mathrm{GL}_2(\mathbb{Z}_n)$ is a group for $n \geq 2$. After a lot of confusion, it turns out $\mathrm{GL}_2(\mathbb{Z}_n)$ is only a group for n a prime integer. This is fairly easy to prove. Let $A, B \in \mathrm{GL}_2(\mathbb{Z}_n)$. Then $\mathrm{GL}_2(\mathbb{Z}_n)$ is a group if and only if $AB \in \mathrm{GL}_2(\mathbb{Z}_n)$. I leae it as an exercise to prove the other requirements for a group, but they will be satisfied for any n. For any integer $0 < a < n$, we can very easily construct a matrix A such that $|A| = a$. Let $0 < a, b < n$, and let $|A| = a$ an $|B| = b$. We thus have $\det(AB) = ab$. Therefore, $AB \in \mathrm{GL}_2(\mathbb{Z}_n)$ if and only if $ab \not\equiv 0 \pmod{n}$. For any n not prime, there exist $a, b \in \mathbb{Z}$ such that this statement is false. Therefore, n must be prime. The conclusion of all this is that the set being over $\mathbb{Z}_n$ literally doesn't matter and this should be provable via normal matrix algebra.

Now, we show the converse. $\square$

Problem 2

Solution. This was easy, in fact we did an example of this last homework. Let $G = \{e, a, b, c\}$ be a group with identity e. Let $a^2 = b^2 = c^2 = e$, and let $ab = ba = c$. It follows that $bc = cb = a$ and $ac = ca = b$. We give the following Cayley table to help with this visualization.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

A great example of an equivalent group up to isomorphism is the subgroup $\{R_0, R_{180}, S, R_{180}S\}$ of the dihedral group D_n for an even integer n.

The group is clearly not cyclic. It has 4 elements, none of which generate the group. Since $a^2 = b^2 = c^2 = e$, we have

$$\langle a \rangle = \{e, a\},$$
$$\langle b \rangle = \{e, b\},$$
$$\langle c \rangle = \{e, c\}.$$

Therefore, the set is not cyclic. Additionally, these sets and the set $\{e\}$ are the only possible cyclic subgroups of G, which is obvious since they are the sets generated by each element of G. It remains to be shown no other subgroups of G exist.

Let $H \subsetneq G$ have more than 2 elements. Since any set must have the identity element in it, we have already seen all the subgroups of G with 2 or less elements. They are exactly the cyclic subgroups of G. We must only consider sets with more than 2 but less than 4 elements. In other words, we must consider sets with only 3 elements. All of these sets, in order to be groups, must have the identity element, so they must have exactly 2 non-identity elements a, b, or c in them. Since $ab = ba = c$, $bc = cb = a$, and $ca = ac = b$, none of these sets would be closed under group multiplication. Thus, there exist no proper subgroups of G other than the cyclic subgroups. □

Problem 3

Solution. □

Problem 4

Solution. Let G be a group with identity e. Let $a, b \in G$ such that $|a| = n$, $|b| = m$, and $\gcd(n, m) = 1$.

Let there exist some $g \in \langle a \rangle$ such that $g \in \langle b \rangle$. Since $g \in \langle a \rangle$, there must exist some $k \in \mathbb{Z}$ such that $g = a^k$. Since $\langle b \rangle$ is a group and thus closed under multiplication, any power of a^k must be an element of $\langle b \rangle$. Thus, we have

$$\left\langle a^k \right\rangle \subseteq \langle b \rangle .$$

By the fundamental theorem of cyclic subgroups, we know that $\left|\left\langle a^k \right\rangle\right|$ will divide m. Additionally, by the same logic $\left\langle a^k \right\rangle \subseteq \langle a \rangle$, so $\left|\left\langle a^k \right\rangle\right|$ must also divide n. Since m and n are relatively prime, the only number that divides both m and n is 1, and thus $\left|\left\langle a^k \right\rangle\right| = 1$. It follows from this that

$$\left(a^k\right)^1 = e.$$

Thus,

$$a^k = e.$$

Therefore, $g \in \langle a \rangle$ and $g \in \langle b \rangle$ implies $g = e$. This should suffice to show $\langle a \rangle \cap \langle b \rangle = \{e\}$. □

Problem 5

Solution. Let $a \in G$. The set $C(a)$ is the set of all $g \in G$ such that $ga = ag$. We need only show $\langle a \rangle \subseteq C(a)$. Since $a^k \in \langle a \rangle$ for any $k \in \mathbb{Z}$, we have

$$a\left(a^k\right) = a\left(a^{k-1}a\right) = \left(aa^{k-1}\right)a = a^k a.$$

Therefore, for any $a^k \in \langle a \rangle$, $a^k a = aa^k$. Thus, $\langle a \rangle \subseteq C(a)$. □