Modern Algebra 1

Grant Talbert
09/19/24
Dr. Duque-Rosero
MA 541 Section A1

Boston University

Problem 1

Solution. (a) $\gcd(12, 40) = 4$. This should be obvious, but I will give some further reasoning because why not. The only divisors of 12 greater than 4 are 6 and 12, and neither of these divide 40.

Since p, q are prime, they have no common divisors. Thus, any divisor of any product of p and q must also be a product of p and q. It should follow that the greatest common divisor is the product of the highest powers of p and q that are in both primes, since any higher power and it would no longer divide one of the numbers. This gives us $\gcd(p^2q^2, pq^3) = pq^2$.

(b) Let $a, b \in \mathbb{Z}$ have $\gcd(a, b) = d$. We know there exist $q_1, r_1 \in \mathbb{Z}$ such that

$$a = q_1 b + r_1$$

and $0 \leq r_1 < |b|$. For $r_1 = 0$, we have $b = d$, since $a = q_1 b$ implies b would divide a, and trivially b divides b. In this case, we are done since

$$d = b = 0a + 1b,$$

and $0, 1 \in \mathbb{Z}$. For $r_1 \neq 0$, we have

$$b = q_2 r_1 + r_2,$$

again with $q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_2 < r_1$. We drop the absolute value signs here, since r_1 is positive, and thus r_2 is also positive. Since $r_1 < |b|$, and $r_2 < r_1$, and $r_1, r_2, b \in \mathbb{Z}$, we have the maximum value of $r_2 = r_1 - 1 = b - 2$. We can repeat this process k times, until $r_k = 0$. At this point, we have

$$r_{k-2} = q_k r_{k-1}.$$

Thus, r_{k-1} divides b. Now, we have to rearrange all of these equations. Since $a = q_1 b + r_1$, we have

$$r_1 = a - q_1 b.$$

We also know that $b = q_2 r_1 + r_2$, so we can plug in for r_1.

$$b = q_2 (a - q_1 b) + r_2 = q_2 a - q_1 q_2 b + r_2.$$

Rearranging, we have

$$r_2 = b - q_2 a + q_1 q_2 b = (1 + q_1 q_2) b - q_2 a.$$

In our next equation, we have

$$r_1 = q_3 r_2 + r_3.$$

We can plug in for r_1 and r_2, and obtain

$$a - q_1 b = q_3 \left((1 + q_1 q_2) b - q_2 a \right) + r_3.$$

It follows that

$$(1 - q_2q_3)a + (q_3 + q_1q_2q_3 - q_1)\, b = r_3.$$

We notice that for any r_i, we can rearrange statements to show that $r_i = pa + qb$ for integers p, q. We continue this process for all k statements, and collect this mess of coefficients into integers m, n. Eventually, we reach

$$r_{k-2} = (ma + nb),$$

since we had $r_k = 0$, and $q_k r_{k-1} = ma + nb$. We can now backtrack. Since $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$, we can plug in our known values, and without loss of generality, absorb the coefficients into our integers m, n. Eventually, we have

$$b = q_2r_1 + r_2 = ma + nb.$$

It follows that, again without loss of generality since we are absorbing into our coefficients,

$$ma = -nb.$$

It follows that $r_{k-1} = d$ or something i dont know i got lost 4 hours ago.

(c) Let $\gcd(a, b) = 1$. By theorem A, it follows that there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Now we prove the converse. Let there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Since 1 is the smallest positive integer, it must be the smallest positive integer that can be written as $ma + nb$. It follows from theorem A that $\gcd(a, b) = 1$. Therefore, a and b are relatively prime if and only if there exist integers $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. □

Problem 2

Solution. (a) Let $a \in \mathbb{Z}^+$. Let $\gcd(a, n) = 1$. By part (c) of problem 1, it follows that there exists integers $x, k \in \mathbb{Z}$ such that $ax + kn = 1$. It should be obvious that $ax + kn \equiv ax \pmod{n}$. Thus, it follows that $ax \equiv 1 \pmod{n}$. Now we prove the converse. Let $ax \equiv 1 \pmod{n}$. It follows that there exists some k such that $ax = 1 + kn$. Thus, $ax - kn = 1$. Without loss of generality, and to avoid having to use negative signs, redefine k such that $ax + kn = 1$. By part (c) of problem 1, since there exist $x, k \in \mathbb{Z}$ such that $ax + kn = 1$, it follows that $\gcd(a, n) = 1$.

(b) Clearly, $U(n)$ is not a subgroup of $\mathbb{Z}_n$, since it is defined under *multiplication* modulo n, not *addition* modulo n. It remains to be shown $U(n)$ is actually a group.

First, we show closure under multiplication modulo n. Let $a, b \in U(n)$. It follows that $\gcd(a, n) = \gcd(b, n) = 1$. From part (c) of problem 1, we have

$$r_1a + k_1n = 1$$

and

$$r_2b + k_2n = 1$$

for $r_1, r_2, k_1, k_2 \in \mathbb{Z}$. We wish to show ab is relatively prime to n. We have

$$\begin{aligned} 1 \cdot 1 &= (r_1a + k_1n)\,(r_2b + k_2n) \\ &= (r_1r_2)\, ab + r_1ak_2n + r_2bk_1n + k_1k_2n^2 \\ &= (r_1r_2)\, ab + (r_1ak_2 + r_2bk_1 + k_1k_2n)\, n. \end{aligned}$$

It follows that there exist integers $\alpha \coloneqq r_1r_2$ and $\beta \coloneqq r_1ak_2 + r_2bk_1 + k_1k_2n$ such that $\alpha ab + \beta n = 1$. Therefore, by part (c) of problem 1, ab is relatively prime to n if a and b are relatively prime to n. It remains to be shown that $ab \pmod{n}$ is relatively prime to n.

By definition, there exists some integers s, λ such that $ab \equiv s + n\lambda \equiv s \pmod{n}$, where we take s to be the minimum possible of the set $\{0, \ldots, n-1\}$. This is an equivalent statement to theorem A, of which part (c) of problem 1 is a special case. Let $\lambda = r_1 aak_2 + r_2 bk_1 + k_1 k_2 n$. It follows that $ab \equiv 1 \pmod{n}$. Thus, $ab \pmod{n}$ is relatively prime to n, and we have closure under multiplication modulo n.

Associativity follows trivially from known properties of the integers. Additionally, $\gcd(1, n) = 1$ for any n, so we have the identity element $1 \in U(n)$. We must show now that inverses exist for any $a \in U(n)$. By part (a) of problem 2, we have for any a relatively prime to n, and thus any $a \in U(n)$, there exists some b such that $ab \equiv 1 \pmod{n}$. We must show such a b is relatively prime to n. Since a is relatively prime to n, and by the logic in the proof of part (a), we have

$$ab + kn = 1.$$

From this, we know there exist integers a, k such that $ab + kn = 1$, and thus $\gcd(b, n) = 1$. Therefore, for any $a \in U(n)$, there exists some $b \in U(n)$ such that $ab = ba = 1$.

(c) By the definition of the function, $|U(n)| = \phi(n)$, where ϕ is the Euler totient function. $\square$

Problem 3

For this problem, for the set X, the notation $|X|$ indicates *the number of elements of* X. This is important to clarify, because although X is probably a subgroup of G, I don't really feel like checking, and we want to avoid ambiguous notation.

Solution. For convenience of notation, let X be the set of all $x \in G$ such that $x^n = e$.

Let $x \in X$. Since $x^n = e$, we have $xx^{n-1} = e$. It follows that $x^{-1} = x^{n-1}$. We also have

$$\left(x^{n-1}\right)^n = x^{n^2-n} = x^{n^2} x^{-n} = (x^n)^n (x^n)^{-1} = e^n e^{-1} = e.$$

Thus, if $x \in X$, then $x^{-1} \in X$.

Now, note that $e^n = e$, and thus $e \in X$. If we can show that for any $x \in X \setminus \{e\}$ that $x \neq x^{-1}$, then we will have finished the proof, because since inverses are unique, we would then have X consisting of *pairs* of elements x, x^{-1}, except for e, which would have no other element to pair with. Since each pair has two elements, we have $|X| = 2n + 1$ for n pairs in X, since there are two elements per pair plus an extra element from e.

Showing that for $x \neq e$, $x \neq x^{-1}$ is actually rather easy. Since n is odd, $n-1$ is even. Since $x = x^1$, and 1 is odd, we have $x^{n-1} \neq x$, since the odd number 1 cannot equal the even number $n-1$. Since $x^{n-1} = x^{-1}$, we have $x \neq x^{-1}$. $\square$

Problem 4

Solution. Obviously, this subgroup will be $H = \{R_0, R_{180}, S, R_{180}S\}$. To show this is true, we must show the following three things:

- $R_{180} \in D_n$ for n even. Since $R_0, S \in D_n$ for any n, the only ambiguity is in R_{180} and $R_{180}S$, both of which can be shown by proving the former. This implies $H \subseteq D_n$.

- H is closed under function composition.

- H is a group.

We begin by proving the first one. A full rotation of any polygon is a rotation by 360 degress. Define R to be the smallest rotation that is an element of D_n. We know that R is a rotation by $360/n$ degrees, so R^n is a rotation by 360 degrees. Since 180 is half of 360, we know $R^{n/2}$ would be a rotation by 180 degrees, if $\frac{n}{2} \in \mathbb{Z}$. Since n is even, it is divisible by 2, and thus $\frac{n}{2} \in \mathbb{Z}$, and thus $R^{\frac{n}{2}} = R_{180} \in D_n$. Since $S \in D_n$, and D_n is a group and thus closed, $R_{180}S \in D_n$.

For the next two points, it suffices to present a Cayley Table.

$\circ$	R_0	R_{180}	S	$R_{180}S$
R_0	R_0	R_{180}	S	$R_{180}S$
R_{180}	R_{180}	R_0	$R_{180}S$	S
S	S	$R_{180}S$	R_0	R_{180}
$R_{180}S$	$R_{180}S$	S	R_{180}	R_0

This table assumes two facts that are worthy of proof:

- $R_{180}S = SR_{180}$.
- $R_{180}SR_{180}S = R_0$.

The second is a corollary of the first. Since $R^iS = SR^{-i}$, we have

$$R_{180}S = R^{\frac{n}{2}}S = SR^{-\frac{n}{2}}.$$

This is a rotation in the opposite direction by 180 degrees. However, a rotation in the opposite direction by 180 degrees is the same as a rotation in the original direction by 180 degrees, so

$$R^{-\frac{n}{2}} = R^{\frac{n}{2}}.$$

Thus,

$$R_{180}S = SR_{180}.$$

By this fact, we have

$$(R_{180}S)(R_{180}S) = (R_{180}S)\,(SR_{180}) = R_{180}(SS)R_{180} = R_{180}R_{180} = R_0.$$

By the same logic, we also have $SR_{180}S = SSR_{180} = R_{180}$. The Cayley table thus clearly shows inverses exist for each element, an identity R_0 exists, the set is closed, and associativity will follow from the fact that D_n is a group. Thus, H is a group. Since $H \subseteq D_n$, H is a subgroup of D_n for any even n. Since H is finite with 4 elements, the order $|H| = 4$. $\square$

Problem 5

This solution makes extensive use of the theorem that for any group G, $H \subseteq G$ is a group if and only if $H \neq \varnothing$, and for any $a, b \in G$, $ba^{-1} \in G$.

Solution. (a) Let G be a group with subgroups H, K. Since $H, K \subseteq G$, we have $H \cap K \subseteq G$. It follows that for the identity element e of G, we have $e \in H$ and $e \in K$, since any group requires an identity element, and thus $e \in H \cap K$. Thus, $H \cap K \neq \varnothing$. It remains to be shown that for $h, g \in H \cap K$, $gh^{-1} \in H \cap K$.

Let $h, g \in H \cap K$. It follows immedately that $h, g \in H$ and $h, g \in K$. Since a set $H \subseteq G$ is a subgroup *if and only if* $h, g \in H$ implies $gh^{-1} \in H$, we thus know $gh^{-1} \in H$ and $gh \in K$ by the reverse direction of this theorem. Since $gh^{-1} \in H$ and $gh^{-1} \in K$, we have $gh^{-1} \in H \cap K$, and thus $H \cap K$ is a subgroup of G.

(b) Since $H \not\subset K$, there must exist at least one $h \in H$ such that $h \notin K$. Conversely, since $K \not\subset H$, there must exist at least one $k \in K$ such that $k \notin H$. We also know tht $k, h \in K \cup H$. Thus, $K \cup H \neq K, H$. By this logic, let $k \in K$ and $h \in H$ such that $k \notin H$ and $h \notin K$. Since H is a subgroup of G, and thus a group, any element of H must have an inverse in H. Therefore, $h \in H$ implies that $h^{-1} \in H$. By this same logic, $h^{-1} \notin K$, since $h^{-1} \in K$ would imply $h \in K$, which is a contradiction. The same logic implies $k^{-1} \in K$ and $k^{-1} \notin H$. We thus have $h, h^{-1}, k, k^{-1} \in H \cup K$.

Now suppose for purpose of contradiction that $H \cup K$ is a group. It follows that since $h, k \in H \cup K$, we have $kh^{-1} \in H \cup K$. As a consequence, at least one of the following two statements are true:

- $kh^{-1} \in H$.
- $kh^{-1} \in K$.

Suppose for now that $kh^{-1} \in H$. Since $kh^{-1}, h \in H$, and since H is a group and thus closed under group multiplication, we have $kh^{-1}h \in H$. It follows that

$$kh^{-1}h = ke = k \in H.$$

This is a contradiction, implying that $kh^{-1} \notin H$.

Now suppose $kh^{-1} \in K$. Again, since $kh^{-1}, k^{-1} \in K$, and since K is a group and thus closed under group multiplication, we have $k^{-1}kh^{-1} \in K$. It follows that

$$k^{-1}kh^{-1} = eh^{-1} = h^{-1} \in K.$$

This is again a contradiction, implying that $kh^{-1} \notin K$.

Since $kh^{-1} \notin K$ and $kh^{-1} \notin H$, we have $kh^{-1} \notin H \cup K$, which is a contradiction since we assumed $H \cup K$ was a group. Thus, $H \cup K$ is not a group, and thus is not a subgroup of G. $\square$