University of Wisconsin-Milwaukee

Modern Algebra

Math 531

Exam 1

Author
Theodore Koss

Supervisor
Dr. Burns Healy

January 19, 2024

1 Problem 1

If a, b are coprime and b, c are coprime, then must a, c be coprime? If so, prove. If not, provide a counterexample. What can you conclude about whether "is coprime to" is an equivalence relation among positive integers. If it is, prove it; if not, declare which axiom it fails.

(a) Consider $a = 2, b = 5, c = 6$. Clearly $\gcd(2, 5) = 1$ and $\gcd(5, 6) = 1$, however, $\gcd(2, 6) = 2$. Thus, a, c are not necessarily coprime when a, b and b, c are.

(b) We can use the above result to prove "is coprime to" is not an equivalence relation over $\mathbb{Z}^+$, because it fails the axiom of transitivity.

2 Problem 2

Let $\mathbb{Z}_k \backslash \{[0]_k\}$ be the set $\mathbb{Z}_k$ without the zero element. What condition on the integer k makes $(\mathbb{Z}_k \backslash \{[0]_k\}, \cdot)$ a group? Prove this condition is both sufficient and necessary.

Proof. k must be a prime number.

- Necessity: $A \implies B$.
  Assume k is prime, then the set $\mathbb{Z}_k \backslash \{[0]_k\}$, with the binary operation $\cdot$, has:

  1. Closure: As $\forall a, b \in \mathbb{Z}_k \backslash \{[0]_k\}$, with prime k, it is impossible to multiply two elements to be equivalent to $[0]_k$.
  2. Identity: The element $[1]_k = e$. Of course.
  3. Inverses: $\forall a \in \mathbb{Z}_k \backslash \{[0]_k\}$, by Bezout's Identity since $\gcd(a, k) = 1$, $\exists x, y \in \mathbb{Z}$ such that $ax + ky = 1$, reduce modulo k to achieve: $ax = 1$. Thus $x \in \mathbb{Z}_k \backslash \{[0]_k\}$ is the inverse of a.
  4. Associativity: Since multiplication over the integers mod k is well defined, $\cdot$ is associative.

  Therefore $(\mathbb{Z}_k \backslash \{[0]_k\}, \cdot)$ is a group.

- Sufficiency: $B \implies A$, or $\neg A \implies \neg B$.
  To the contrary, assume k is composite. Then $k = pq$, for some $p, q \neq 1 \in \mathbb{Z}_k \backslash \{[0]_k\}$. This shows that there exists some $a, b \in \mathbb{Z}_k \backslash \{[0]_k\}$ such that $ab = k \equiv [0]_k \notin \mathbb{Z}_k \backslash \{[0]_k\}$. Thus $(\mathbb{Z}_k \backslash \{[0]_k\}, \cdot)$ is not closed, and is therefore not a group. As required.

QED

3 Problem 3

Prove that, for an arbitrary integer $n \geq 2$, any integer M can be written as $m = an + r$, where $a \in \mathbb{Z}$ and $2n \leq r < 3n$.

Proof. To show existence, we consider some set

$$S = \{m - an = r | a \in \mathbb{Z}\}, m - an \geq 0$$

If we can prove this set is nonempty, by the well ordering principle, there will be a least element. There are two cases for r.

(i) $m \geq 0$, in this case, we set $a = 0$ and achieve the following: $r = m - 0n = m \in S$.

(ii) $m < 0$, then we can set $a = m$. Then $r = m - an = m - mn = m(1-n)$. And since $m < 0$ and $n \geq 2$, $a(1-d)$ is, of course, an element of S.

Thus S is nonempty, and therefore has a least element $r = m - an$, rearranging this we get our original equation must be true: $m = an + r$.
However this does not show uniqueness of a and r. To prove this, consider some elements b, s (haha, get it?) satisfy $m = bn + s$. Then, we may assume $s \geq r$, and thus, $0 \leq r - s < n$. Since $m = bn + s = an + r$, the following holds:

$$r - s = n(b - a)$$

Which, by definition, means n divides $r - s$, which implies either $r - s \geq d$ or $r - s = 0$. But, since we know $0 \leq r - s < n$, $r - s = 0$ and therefore $r = s$. This, of course, implies $b = a$, therefore r and a are unique. QED

4 Problem 4

Let k, n be arbitrary positive integers. Find a matrix M_k that has order k as an element of the group $GL_n(\mathbb{C})$.

Proof. $GL_n(\mathbb{C}) = \{A = [a_{ij}]_{n\times n}\}$, such that $|A| \neq 0$ and $a_{ij} \in \mathbb{C}$. This is the group of matrices of $n \times n$ order, with nonzero determinants.
Thus, upper or lower triangular matrix will have determinant $|A| = \underbrace{a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}}_{\text{Product of diagonal elements.}}$, which will of course be nonzero, since all of $a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}$ are nonzero. QED

5 Problem 5

Let P, Q be regular polygons. Let G_P, G_Q be the group of rigid motions of P, Q, respectively. Show that if there is an isomorphism between G_P, G_Q, then the polygons are similar. Do they also have to be congruent?

Proof. Consider the regular polygons P, Q, and consider the polygon to be a n-gon, and m-gon respectively. Then $G_P = D_n$, and $G_Q = D_m$. Therefore the order of the rigid motion groups G_P, G_Q are $2n$, and $2m$, respectively (This is proven in problem 7). Since $|G_P|, |G_Q| \neq \infty$, in order for there to be an isomorphism $\phi : G_P \to G_Q$, $|G_P| = |G_Q|$. Therefore, $2m = 2n$, this necessarily implies $m = n$. And by this result in geometry, all regular simple polygons with the same number of sides are similar. Thus, P must be similar to Q if there exists an isomorphism between their respective groups. However, this result has nothing to do with the congruence of these two polygons.

Counterexample: consider P to be some regular 4-gon with area 4, whose rigid motion group is isomorphic to some other rigid motion group of a polygon, Q, with area 25. Then, by our result above, Q must also be a square (regular 4-gon). These two rigid motion groups are isomorphic, however clearly, $4 \neq 25$ and therefore they are not congruent.

So if there exists an isomorphism between rigid motion groups G_P and G_Q for regular polygons P and Q, then P and Q must be similar, however they do not necessarily have to be congruent. QED

6 Problem 6

Define $\mathbb{C}_r$ to be the set $\{a + rbi | a, b \in \mathbb{R}\}$ for each $r \in \mathbb{R}$.

- Prove that this set is a group under addition.

  Proof. To be a group, the following must be true:

  (a) Closure: This holds because $\forall n, m \in \mathbb{C}_r$, where $n = a_n + rb_n i$, and $m = a_m + rb_m i$, their sum, $n + m = \underbrace{a_n + a_m}_{\text{Real part}} + \underbrace{ri(b_n + b_m)}_{\text{Imaginary part}} \in \mathbb{C}_r$.

  (b) Existence of identity: The identity element is 0, $n + 0 = n$.

  (c) Existence of inverses: For each element $n = a_n + rb_n i$, the inverse is $n^{-1} = -a_n - rb_n i \in \mathbb{C}_r$. Therefore every element has inverses.

  (d) Associativity of addition, this holds because $\forall n, m, l \in \mathbb{C}_r$, $n + (m + l) = (n + m) + l$.

  Thus, $(\mathbb{C}_r, +)$ is a group. QED

- For what values of r are the groups $(\mathbb{C}, +)$ and $(\mathbb{C}_r, +)$ isomorphic?

  Proof. All values $r \in \mathbb{R}$. This is the case because we can set up a bijective homomorphism $\phi : (\mathbb{C}_r, +) \to (\mathbb{C}, +)$ defined by $\phi(n \in \mathbb{C}_r) = m \in \mathbb{C}$. $\forall n = a_n + rb_n i \in \mathbb{C}_r$, the homomorphism $\phi : (\mathbb{C}_r, +) \to (\mathbb{C}, +)$ is rather trivial, as to define a unique element $m = a_m + b_m i \in \mathbb{C}$, simply let $a_m = a_n$ and $b_m = rb_n$. To show ϕ is a bijection, we N2S the following:

  (a) ϕ is injective. This is the case because if we choose some value k for which $\phi(k) = \phi(n) = m$, this means $k = a_k + rb_k i = m \in \mathbb{C}$, but so does $n = a_n + rb_k i$. Which implies that $a_m = a_k = a_n$, and $b_m = rb_k = rb_n$ This shows if there did exist some k, n for which $\phi(k) = \phi(n)$, it would imply that $k = n$.

  (b) ϕ is surjective. This is also true because $\forall m = a_m + b_m i \in \mathbb{C}$, $\exists n \in \mathbb{C}_r$ s.t. $\phi(n) = m$, specifically defined by $n = a_n + rb_n i$ where $a_m = a_n$ and $b_m = rb_n$.

  QED

7 Problem 7

Define the order of a group. Let D_n be the dihedral group and let Sym_n be the symmetric group on n letters. State and prove a relationship between $|D_n|$ and $|Sym_n|$.
The order of a group is the cardinality (or "size") of the group. The relationship between the orders of D_n and Sym_n is $\dfrac{|Sym_n|}{|D_n|} = \dfrac{n!}{2n}$.

Proof. For Sym_n, the permutation group is a bijection from a set of n elements to itself. Therefore, if you choose some $a \in Sym_n$, it has n choices to be sent to, then the next element $b \in Sym_n$ has $n-1$ choices to be sent to. Continue this for all elements of Sym_n, and the result is $|Sym_n| = n!$.
For D_n, this is the group of symmetries of a regular n-gon. WLOG, consider the example $n = 3$. This is the group of symmetries of an equilateral triangle. By inspection, it is easy to see that a rotation by $\frac{360}{3}^\circ$ is a symmetry, in fact, a symmetry for each rotation up to $360^\circ = e$, in this case 3. We can generalize this to any n-gon to get the first n symmetries. The next n symmetries come from drawing a line through one of the n vertices, then reflecting the shape over this line. Do this for each vertex to get n more symmetries. The final result is $n + n = 2n$ symmetries of a regular n-gon, and therefore $|D_n| = 2n$. QED

8 Problem 8

Prove that differentiable, bijective functions from $\mathbb{R} \to \mathbb{R}$ form a group under composition.

Proof. Let $G = \{\text{Bijections } \phi : \mathbb{R} \to \mathbb{R}\}$. N2S: $(G, \circ)$ is a group, where $\circ$ denotes function composition.

1. Closure: A bijection composed with a bijection is necessarily another bijection, therefore G is closed under composition.

2. Identity: The element $e = \phi$ where $\phi(x) = x$ is the identity function, and $e \in G$.

3. Inverses: For each element $\phi \in G$, ϕ defines some bijection from $\mathbb{R} \to \mathbb{R}$, then there must exist another bijection θ, where θ defines a bijection

from $\mathbb{R} \to \mathbb{R}$. WLOG, as an example, consider the finite sets $X = \{1, 2, 3\}$ and $Y = \{-1, -2, -3\}$. Of course, a bijection ϕ exists, namely $\phi : X \to Y$ defined by $\phi(x) = -x$, $\forall x \in X$. There also exists a bijection $\theta : Y \to X$, defined by $\theta(y) = -y$, $\forall y \in Y$. This θ is the inverse of ϕ, this also means $\phi \circ \theta = e$. We can see this because if we do the bijection ϕ, it's the mapping $1 \to -1, 2 \to -2, 3 \to -3$, then θ is the mapping $-1 \to 1, -2 \to 2, -3 \to 3$. Therefore composing the two is the same as doing nothing. This case can be generalized to the infinite set $\mathbb{R}$.

4. Associativity: Function composition is associative.

QED