Midterm 1
Abstract Algebra
Math 320
Stephen Giang, Emily Boyd
Bennett Guillaume, Dacia Bond

Problem 1:

(a) Let $q > 0$ be prime. Prove that for $1 \le s \le q-1, q$ divides $\binom{q}{s}$, where $\binom{q}{s} = \frac{q!}{s!(q-s)!}$. You may assume $\binom{q}{s}$ is an integer.

Solution. Let $q > 0$ and be prime and $1 \le s \le q-1$

$$\binom{q}{s} = \frac{q!}{s!(q-s)!}$$

$$q! = \binom{q}{s}(s!(q-s)!)$$

$$q \left| \prod_{k=0}^{q} q-k \right. \text{ so } q|q!$$

$$q|q! = q \left| \binom{q}{s}(s!(q-s)!) \right.$$

$$\text{By Corrollary 1.6: } q \left| \binom{q}{s} \right. \text{ or } q|(s!(q-s)!)$$

Because s and $(q-s) < q$, their prime factorization doesn't contain q, so $q \nmid (s!(q-s)!)$. Thus q has to divide $\binom{q}{s}$

□

(b) Let $q > 0$ be prime. Prove that for any $\beta, \gamma \in \mathbb{Z}_q, (\beta+\gamma)^q = \beta^q + \gamma^q$ in $\mathbb{Z}_q$

Solution. Let $q > 0$ and be prime and $\beta, \gamma \in \mathbb{Z}_q$

By Binomial Therorem:

$$(\beta+\gamma)^q = \beta^q + \left(\sum_{k=1}^{q-1} \binom{q}{k} \beta^{q-k}\gamma^k\right) + \gamma^q$$

$$\text{Because } q \left| \binom{q}{s} \right. \text{ with } 1 \le s \le q-1$$

$$q \left| \binom{q}{k} \right., \text{ which means that } \left[\binom{q}{k}\right] = [0]_q \qquad 1 \le k \le q-1$$

$$\text{So } (\beta+\gamma)^q = \beta^q + \left(\sum_{k=1}^{q-1} (0)\beta^{q-k}\gamma^k\right) + \gamma^q$$

Thus for any $\beta, \gamma \in \mathbb{Z}_q, (\beta+\gamma)^q = \beta^q + \gamma^q$ in $\mathbb{Z}_q$

□

Problem 2:

(a) Let $x, y, z \in \mathbb{Z}$. If $x|z$ and $y|z$ and $(x, y) = w$, prove that $xy|wz$

Solution. Let $x, y, z \in \mathbb{Z}$ with $x|z$ and $y|z$ and $(x, y) = w$

$$\begin{aligned} z &= xa = yb \\ w &= xu + yv \\ wz = w(xa) &= xa(xu + yv) \\ &= xaxu + xayv \\ &= ybxu + xayv \\ &= xy(bu + av) \end{aligned}$$

Because wz can be written as a product of an integer and xy, $xy|wz$

$\square$

(b) Suppose χ and ρ are primes, and $\chi, \rho \geq 5$. Prove that $24|(\chi^2 - \rho^2)$

Solution. Let χ and ρ are primes, and $\chi, \rho \geq 5$. Let $q_1, q_2, k_1, k_2 \in \mathbb{Z}$

Notice: χ^2 prime factorization: $1, \chi$
Notice: ρ^2 prime factorization: $1, \rho$
Because $\chi \geq 5$ and prime , $(\chi^2, 3) = 1$ & $(\chi^2, (2)(2)(2)) = 1$
Because $\rho \geq 5$ and prime , $(\rho^2, 3) = 1$ & $(\rho^2, (2)(2)(2)) = 1$

If ρ or $\chi = \{3k + 1, \quad 3k + 2, \quad 8k + 1, \quad 8k + 3, \quad 8k + 5, \quad 8k + 7\}$, then $\chi^2 = \{3q_1 + 1, \quad 8k_1 + 1\}$ and $\rho^2 = \{3q_2 + 1, \quad 8k_2 + 2\}$

$$\begin{aligned} \chi^2 = 3q_1 + 1 \quad \rho^2 &= 3q_2 + 1 \\ (\chi^2 - \rho^2) &= 3(q_1 - q_2) \\ 3|(\chi^2 - \rho^2) \end{aligned} \qquad\qquad \begin{aligned} \chi^2 = 8k_1 + 1 \quad \rho^2 &= 8k_2 + 1 \\ (\chi^2 - \rho^2) &= 8(k_1 - k_2) \\ 8|(\chi^2 - \rho^2) \end{aligned}$$

From part (A), because $3|(\chi^2 - \rho^2)$ and $8|(\chi^2 - \rho^2)$ with $(8, 3) = 1$, $24|(\chi^2 - \rho^2)$

$\square$

Problem 3:

(a) Prove that if $\mu, \nu \in \mathbb{Z}$ and $(\mu, \nu) = 1$, then $(\mu + \nu, \nu) = 1$

Solution. Let $\mu, \nu, q \in \mathbb{Z}$ and $(\mu, \nu) = 1$, Let $d|(\mu + \nu)$ and $d|\nu$

$$\begin{aligned}
&\nu = dk && \text{for some k} \in \mathbb{Z} \\
&\mu + \nu = dq && \text{for some q} \in \mathbb{Z} \\
&\mu = dq - dk = d(q - k) \\
&d|\mu
\end{aligned}$$

Because $d|\mu$ and $d|\nu$, the only d to divide $\mu, \nu, \mu + \nu$ is 1, thus $(\mu + \nu, \nu) = 1$ □

(b) Prove that if $\mu, \nu \in \mathbb{Z}$ and $(\mu, \nu) = 1$, then $(\mu + \nu, \nu^n) = 1$

Solution. Let $\mu, \nu, q \in \mathbb{Z}$ and $(\mu, \nu) = 1$ for $n \geq 1$

Because μ and ν dont share any prime factors, μ and ν^n wont share any prime factors as ν^n will consist of multiple ν's that again dont share any prime factors with μ.

$$(\mu, \nu^n) = 1$$

We know from part (a), that because $(\mu, \nu) = 1, (\mu + \nu, \nu) = 1$ If we let d divide $\mu + \nu$ and ν, then d divides μ. And because d divides ν, it divides ν^n. So because d divides μ and ν^n, d has to be one, meaning $(\mu + \nu, \nu^n) = 1$ □

(c) Let q be prime, and $\mu, \nu \in \mathbb{Z}_{>0}$ such that $(\mu, \nu) = 1$. Prove that

$$\left(\mu + \nu, \frac{\mu^q + \nu^q}{\mu + \nu}\right) = 1 \text{ or } q$$

(i) Notice: $\mu^q = ((\mu + \nu) - \nu)^q$

$$\begin{aligned}
\mu^q + \nu^q &= ((\mu + \nu) - \nu)^q + \nu^q \\
&= \left(\sum_{k=0}^{q} \binom{q}{k} (\mu + \nu)^{q-k} (-\nu)^k\right) + \nu^q \\
&= \left(\sum_{k=0}^{q-1} \binom{q}{k} (\mu + \nu)^{q-k} (-\nu)^k\right) + (-\nu)^q + \nu^q
\end{aligned}$$

Notice: q cannot be even, because it is prime, so $(-\nu)^q = -\nu^q$

$$\begin{aligned}
&= \sum_{k=0}^{q-1} \binom{q}{k} (\mu + \nu)^{q-k} (-\nu)^k \\
\frac{\mu^q + \nu^q}{\mu + \nu} &= \frac{1}{\mu + \nu} \sum_{k=0}^{q-1} \binom{q}{k} (\mu + \nu)^{q-k} (-\nu)^k \\
&= \sum_{k=0}^{q-1} \binom{q}{k} (\mu + \nu)^{q-1-k} (-\nu)^k
\end{aligned}$$

Because integers are closed under $(+)$ and $(\times)$, $\frac{\mu^q + \nu^q}{\mu + \nu} \in \mathbb{Z}$

(ii) Let $d = \left(\mu+\nu, \frac{\mu^q+\nu^q}{\mu+\nu}\right)$, so $d|\frac{\mu^q+\nu^q}{\mu+\nu}$, $d|(\mu+\nu)$ and Let $a, b, c \in \mathbb{Z}$

$$\begin{aligned} da &= \frac{\mu^q+\nu^q}{\mu+\nu} \\ &= \sum_{k=0}^{q-1} \binom{q}{k} (\mu+\nu)^{q-1-k}(-\nu)^k \\ &= \left(\sum_{k=0}^{q-2} \binom{q}{k} (\mu+\nu)^{q-1-k}(-\nu)^k\right) + q(-\nu)^{q-1} \end{aligned}$$

Because $d|(\mu+\nu)$, $d|(\mu+\nu)^z$ for $z \in \mathbb{Z}^+$, so

$$d\left|\sum_{k=0}^{q-2} \binom{q}{k} (\mu+\nu)^{q-1-k}(-\nu)^k,\right. \qquad \sum_{k=0}^{q-2} \binom{q}{k} (\mu+\nu)^{q-1-k}(-\nu)^k = db$$

$$\begin{aligned} da - db &= q(-\nu)^{q-1} \\ dc &= q(-\nu)^{q-1} \end{aligned}$$

Because q is prime, q is odd, such that (q-1) is even, so

$$dc = q\nu^{q-1}$$

Thus, $d|q\nu^{q-1}$

(iii) Notice from part (b): $(\mu+\nu, \nu^{q-1}) = 1$. This means $\mu+\nu$ and ν^{q-1} don't share any factors except 1. Because d is a factor of $\mu+\nu$, d is not a factor of ν^{q-1}, unless $d = 1$. Thus $(d, \nu^{q-1}) = 1$

(iv) Because $(d, \nu^{q-1}) = 1$ and $d|q\nu^{q-1}$, $d|q$ by Theorem 1.4, if d divides a prime, q, d = 1 or q, so:

$$\left(\mu+\nu, \frac{\mu^q+\nu^q}{\mu+\nu}\right) = 1 \text{ or } q$$

Problem 4: Let L be the set of positive real numbers. Define alternate addition and multiplication operations on L by

$$a \oplus b = ab \qquad\qquad a \otimes b = a^{\ln b}$$

(a) Prove or disprove: L is commutative.

Solution. Let $a \otimes b = y = a^{\ln b}$, and $b \otimes a = x = b^{\ln a}$

$$\begin{aligned} y &= a^{\ln b} \\ \ln y &= \ln a^{\ln b} \\ &= \ln b \ln a \end{aligned} \qquad\qquad \begin{aligned} x &= b^{\ln a} \\ \ln x &= \ln b^{\ln a} \\ &= \ln a \ln b \end{aligned}$$

Because multiplication of real numbers is commutative, $\ln b \ln a = \ln a \ln b$, so $\ln y = \ln x$, which means that $y = a \otimes b = x = b \otimes a$, thus L is commutative. □

(b) Find the multiplicative identity of L.

Solution. Let x be the multiplicative identity, 1_L, such that $a \otimes x = a$

$$\begin{aligned} &a \otimes x = a^{\ln x} \\ &\text{Because } a \otimes x = a \qquad 1 = \ln x \end{aligned}$$

Thus the multiplicative identity, $x = 1_L = e$

□

(c) Prove that L is a field

Solution. From part (b): $1_L = e$, let x be denoted as the multiplicative inverse of a such that $a \otimes x = 1_L$

$$\begin{aligned} &a \otimes x = 1_L \\ &a^{\ln x} = e \\ &\ln x \ln a = 1 \\ &x = e^{1/\ln a} \text{ or } e^{\log_a(e)} \end{aligned}$$

Because $\forall a \in L, \exists x$ such that $a \otimes x = 1_L$, L is a field. □

Problem 5: Let S be a set, and let 2^S denote the power set of S, i.e. the set of all subsets of S. Define addition and multiplication in 2^S by the rules:

$$M + N = (M - N) \cup (N - M), \qquad\qquad MN = M \cap N$$

where

$$M - N = M \backslash N = \{x \in S : x \in M, x \notin N\}$$

Under these operations, we may assume that 2^S is a ring.

(a) Show that S is the multiplicative identity of this ring.

Solution. Let $M \in 2^S$ and represent any arbitrary element of 2^S

$$MS = M \cap S = M$$

Thus by the definition of multiplicative identity, S is the multiplicative identity

$\square$

(b) Show that the empty set $\emptyset$ is the additive inverse of 2^S

Solution. Let $M \in 2^S$ and represent any arbitrary element of 2^S

$$M + \emptyset = (M - \emptyset) \cup (\emptyset - M) = M \cup \emptyset = M$$

Thus by the definition of the additive inverse, $\emptyset$ is the additive inverse of 2^S

$\square$

(c) Prove that if $T \in 2^S$ and $T \subsetneq S$, then T is not a unit in 2^S.

Solution. Let $T, R \in 2^S$ and $T, R \subsetneq S$

$$TR = T \cap R.$$

Because $[T, R \subsetneq S], [T \cap R \subsetneq S]$, which means $TR \neq S$ thus T is not a unit

$\square$

(d) Prove that under these operations, 2^S is an integral domain iff $|S| = 1$

$\rightarrow$. Contrapositive: "If $|S| \neq 1$, then 2^S is not an integral domain"
Let $|S| \neq 1$
Case 1: $|S| < 1$

$$\text{So } |S| = 0, S = \emptyset$$

For 2^S to be an integral domain, there has to be 2 nonzero elements that multiply to equal 0. But because S doesn't have any nonzero elements, 2^S is not an integral domain

Case 2: $|S| > 1$, Let $(M - N), (N - M) \in 2^S$ with (M-N),(N-M) both being nonzero elements.

$$(M - N)(N - M) = (M - N) \cap (N - M) = \emptyset \tag{1}$$

Because both of them are not the zero element, the ring is not an integral domain.

Because for $|S| \neq 1$, the result of 2^S not being an integral domain holds true. So by contraposition, if 2^S is an integral domain, then $|S| = 1$

$\square$

$\leftarrow$. Let $|S| = 1$, so let $A, B \in 2^S$

$$\text{Because } |S| = 1, A = \emptyset \text{ and } B = S \text{ or } A = S \text{ and } B = \emptyset$$

So $A = \emptyset$ or S. In any case, $AB = \emptyset$ with A or B = $\emptyset$.

$\square$

Problem 6: An element a of a ring is called nilpotent if $a^n = 0_R$ for some postive integer n.

(a) Let a and b be nilpotent elements in a commutative ring R. Prove that $a + b$ and ab are also nilpotent.

Solution. Let a and b be nilpotent elements in a commutative ring R

$$(a+b)^n = \sum_{k=0}^{n} a^{n-k}b^k = \sum_{k=0}^{n} 0_R 0_R = 0_R$$
$$(ab)^n = a^n b^n = 0_R 0_R = 0_R$$

Thus $a + b$ and ab are also nilpotent

$\square$

(b) Prove that if a is a nilpotent element of ring R, then $-a$ is also nilpotent.

Solution. Let a be nilpotent in R
Case 1) n is even

$$(-a)^n = a^n = 0_R$$

Case 2) n is odd

$$(-a)^n = -a^n = -0_R = 0_R$$

Thus $-a$ is also nilpotent $\square$

(c) Let N be the set of all nilpotent elements of a commutative ring R. Show that N is a subring of R.

Solution. Let N be the set of all nilpotent elements of a commutative ring R.

$$(a+b)^n = \sum_{k=0}^{n} a^{n-k}b^k = \sum_{k=0}^{n} 0_R 0_R = 0_R \in N$$
$$(a-b)^n = \sum_{k=0}^{n} a^{n-k}(-b)^k = \sum_{k=0}^{n} 0_R 0_R = 0_R \in N$$
$$(ab)^n = a^n b^n = 0_R 0_R = 0_R \in N$$
$$0^n = 0_R \in N$$

Because of closure under addition,subtraction,multiplication and containing 0_N, N is a subring of R $\square$

Problem 7: (a) If R, S are rings such that $R \cong S$, then $S \cong R$

Solution. Let R, S be rings such that $R \cong S$. So $f : R \to S$ with f being bijective and holding the homomorphism properties. Let $g : S \to R$

Let $x \in R$ and $y \in S$ $\qquad f(x) = y \qquad g(y) = g(f(x)) = x$

Let: $g(f(x_1)) = g(f(x_2))$
$x_1 = x_2$
Thus $f(x_1) = f(x_2)$, and g is injective

Notice: $g(f(x)) = x$
Because f is surjective, for all $x \in R,$ there exists an $f(x)$ such that $g(f(x)) = x,$
Thus g is surjective.

Notice: $f(x_1 + x_2) = f(x_1) + f(x_2)$
$g(f(x_1) + f(x_2)) = g(f(x_1 + x_2)) = x_1 + x_2$
$g(f(x_1)) + g(f(x_2)) = x_1 + x_2$

Notice: $f(x_1x_2) = f(x_1)f(x_2)$
$g(f(x_1)f(x_2)) = g(f(x_1x_2)) = x_1x_2$
$g(f(x_1))g(f(x_2)) = x_1x_2$

Because g is bijective and holds the homomorphism properties, $S \cong R$ $\square$

Problem 8: Let C be the set $\mathbb{R} \times \mathbb{R}$ with the usual coordinate addition and a new multiplication given by

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

Under these operations, $\mathbb{R} \times \mathbb{R}$ is a field.

(a) Find the multiplicative identity of C and show that every nonzero element (a, b) has a multiplicative inverse in C.

Solution. Find (x, y) such that $(a, b)(x, y) = (ax - by, ay + bx) = (a, b)$ (Read Left to Write for Elimination Steps)

$$1) ax - by = a \qquad 2) ax - by = a \qquad 3) ax - by = a$$

$$bx + ay = b \qquad \frac{-a}{b}(bx + ay = b) \qquad -ax - \frac{a^2}{b}y = -a$$

$$-y(b + \frac{a^2}{b}) = 0 \qquad -y(b^2 + a^2) = 0 \qquad y = 0$$

By repluggin in $y = 0$, we get $x = 1$, so then the multiplicative identity is (1,0) □

Solution. Find (x, y) such that $(a, b)(x, y) = (ax - by, ay + bx) = (1, 0)$ (Read Left to Write for Elimination Steps)

$$1) ax - by = 1 \qquad 2) ax - by = 1 \qquad 3) ax - by = 1$$

$$bx + ay = 0 \qquad \frac{-a}{b}(bx + ay = 0) \qquad -ax - \frac{a^2}{b}y = 0$$

$$-y(b + \frac{a^2}{b}) = 1 \qquad -y(b^2 + a^2) = b \qquad y = \frac{-b}{b^2 + a^2}$$

By replugging in $y = \frac{-b}{b^2+a^2}$, we get $x = \frac{a}{b^2+a^2}$, so then the multiplicative inverse is

$$\left(\frac{a}{b^2 + a^2}, \frac{-b}{b^2 + a^2}\right)$$

□

(b) Prove that C $\cong \mathbb{C}$

Solution. Define f as f: C $\rightarrow \mathbb{C}$

$$\text{Let } f((a,b)) = f((c,d)) \tag{2}$$
$$f((a,b)) = a + bi = f((c,d)) = c + di \tag{3}$$

Because $f((a,b)) = f((c,d)), a = c, b = d$ such that $(a,b) = (c,d)$, so f is injective

$$\text{Let } y = a + bi$$

If we set $x = (a,b)$. Thus there exists an x, that satisfies $f(x) = y$ for all $y \in \mathbb{C}$. So f is surjective.

$$f((a,b) + (c,d)) = f((a+c, b+d)) = (a+c) + (b+d)i$$
$$f((a,b)) + f((c,d)) = (a+c) + (b+d)i$$

$$f((a,b)(c,d)) = f((ac-bd, ad+bc)) = (ac-bd) + (ad+bc)i$$
$$f((a,b))f((c,d)) = (a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

Because the homomorphism properties hold, along with the function f is bijective, $C \cong \mathbb{C}$

□

Problem 9:

(a) Show that $\mathbb{Z}$ and $\mathbb{Q}$ both have characteristic zero, and that $\mathbb{Z}_n$ has a characteristic n

Solution. Notice: $1_{\mathbb{Z}} = 1_{\mathbb{Q}} = 1$ and $0_{\mathbb{Z}} = 0_{\mathbb{Q}} = 0$ and $1_{\mathbb{Z}_n} = [1]_n$ and $0_{\mathbb{Z}_n} = [0]_n$. Let x denote the solution of $x1_R = 0_R$

$$\begin{aligned} x(1) &= 0 \\ \frac{x(1)}{1} &= \frac{0}{1} \\ x &= 0 \end{aligned} \qquad\qquad \begin{aligned} [x]_n[1]_n &= [0]_n \\ [x]_n &= [0]_n \\ x &= n \end{aligned}$$

Thus $\mathbb{Z}$ and $\mathbb{Q}$ both have characteristic zero and $\mathbb{Z}_n$ has a characteristic n

□

(b) What is the characteristic of $A = M_2(\mathbb{Z}_2) \times \mathbb{Z}_3$

Solution. Notice $1_A = \left(\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, [1]_3\right)$ and $0_A = \left(\begin{pmatrix} [0]_2 & [0]_2 \\ [0]_2 & [0]_2 \end{pmatrix}, [0]_3\right)$.
Let x denote the solution to $x1_A = 0_A$

$$x\left(\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, [1]_3\right) = \left(\begin{pmatrix} [0]_2 & [0]_2 \\ [0]_2 & [0]_2 \end{pmatrix}, [0]_3\right)$$

Because the characteristic of $M_2(\mathbb{Z}_2)$ is $\begin{pmatrix} [2]_2 & [2]_2 \\ [2]_2 & [2]_2 \end{pmatrix}$, and the characteristic of $\mathbb{Z}_3$ is 3, and by properties of multiplication under Cartesian Product of Rings, the characteristic of $A = \left(\begin{pmatrix} [2]_2 & [2]_2 \\ [2]_2 & [2]_2 \end{pmatrix}, 3\right)$ □

(c) Prove that the characteristic of an integral domain D must either be 0 or a prime p.

Solution. Let the characteristic of D be a composite number, n.

$n = mk$

$n1_D = 0_D$

$(m1_D)(k1_D) = 0_D$

Because D is an integral domain, either $m1_D = 0_D$ or $k1_D = 0$

If either is true, then n would not be smallest positive integer that satisfies $n1_D = 0_D$, thus n cannot be composite by contradiction.

Let the characteristic of D be 1_D
This would be impossible because this would contradict the definition of the multiplicative identity.

Because the characteristic is the smallest positive number, n, and we have proved it can't be 1 or composite for all integral domains, D, the characteristic is either 0 or prime p.

□

Problem 10:

(a) Prove that $\mathbb{Z}$ and $M_3(\mathbb{Z}_2)$ are not isomorphic.

Solution. Define f: $\mathbb{Z} \to M_3(\mathbb{Z}_2)$ such that for some $a \in \mathbb{Z}$, $f(a) = \begin{pmatrix} [a]_2 & [a]_2 & [a]_2 \\ [a]_2 & [a]_2 & [a]_2 \\ [a]_2 & [a]_2 & [a]_2 \end{pmatrix}$.

$$\text{Notice: } f(0) = f(2) = f(4) = \begin{pmatrix} [0]_2 & [0]_2 & [0]_2 \\ [0]_2 & [0]_2 & [0]_2 \\ [0]_2 & [0]_2 & [0]_2 \end{pmatrix}$$

This means that f is not injective, thus proving that $\mathbb{Z} \ncong M_3(\mathbb{Z}_2)$

$\square$

(b) Prove that $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_8$ are not isomorphic

Solution. Define f: $\mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_8$ such that for some $a, b \in \mathbb{Z}$, $f(([a]_4, [b]_2)) = [ab]_8$

$$f([1]_4, [2]_2) = f([1]_4, [0]_2)$$
$$f([1]_4, [2]_2) = [2]_8$$
$$f([1]_4, [0]_2) = [0]_8$$

Because $[2]_8 \neq [0]_8$, f is not injective, thus $\mathbb{Z}_4 \times \mathbb{Z}_2 \ncong \mathbb{Z}_8$ $\square$