

Test 2 Due April 22, 2008

1. If R is a ring, then $M_n(R)$ is the ring of $n \times n$ matrices with coefficients in R . $R[x]$ is the ring of polynomials whose coefficients are in R . If R_1, R_2, \dots, R_n are n rings, not necessarily different, $\prod_{i=1}^n R_i$ is the product ring. In the questions below, you can find examples among the types of rings described above. Furthermore, it suffices to use \mathbb{Z} , $n\mathbb{Z}$ or \mathbb{Z}_n for R .

Give examples of

- (a) Two non-commutative rings without unities, one with zero divisors and one without.
For any integers $n > 1$ and $m > 1$, $R = M_n(m\mathbb{Z})$ is a non-commutative ring without unity. In particular, 2×2 matrices with even integers as elements constitute such a ring. Comment: Not only do rings of matrices contain zero divisors, they contain “nilpotent” elements. A non-zero element, a , of a ring is called “nilpotent” if $a^n = 0$ for some $n > 1$. Any $n \times n$ matrix whose only non-zero elements are above the main diagonal ($a_{i,j} = 0$ if $i \geq j$) is nilpotent.
For any integral $n > 1$, $R = \{a + bi + cj + dk \mid a, b, c, d \in n\mathbb{Z}\}$ is a non-commutative ring without unity. The quaternions are isomorphic to a subring of $M_2(\mathbb{C})$, as discussed in class and as outlined in problem 24.19 (page 227). Thus, the example can be restated as:

$$R = \left\{ \begin{pmatrix} a + di & b + ci \\ -b + ci & a - di \end{pmatrix} \mid a, b, c, d \in n\mathbb{Z} \right\}.$$

- (b) Two commutative rings with unities, one with zero divisors and the other without.
SOLUTION: \mathbb{Z} is a commutative ring with unity, 1. $\mathbb{Z} \times \mathbb{Z}$ is a commutative ring with unity, $(1, 1)$. \mathbb{Z} has no zero divisors and $\mathbb{Z} \times \mathbb{Z}$ has. For example, $(1, 0) \cdot (0, 1) = (0, 0)$.

- (c) An infinite ring with characteristic 13.
SOLUTION: $\mathbb{Z}_{13}[x]$ is an infinite ring with characteristic 13.

- (d) An infinite ring with characteristic 0 that has a subring of characteristic 10.
SOLUTION: $\mathbb{Z}_{10} \times \mathbb{Z}$ is an infinite ring with characteristic 0. The subring generated by $(1, 0)$ is a finite sub-ring with characteristic 10.

- (e) An ideal that is not principal in a commutative ring with unity.
SOLUTION:
In $\mathbb{Z}[x]$, let N_1 be the ideal generated by 5 and x . That is, a polynomial, $f(x) \in N_1$ if and only if its constant term is a multiple of 5. If N_1 were a principal ideal, then it would be generated by some polynomial, $p(x) = a_0 + a_1x + \dots + a_nx^n$. Since the constant polynomial, 5, is in N_1 , $5 = q(x)p(x)$ for some polynomial, $q(x)$. This means that the degrees of $p(x)$ and $q(x)$ must both be 0, so $q(x) = b$ for some integer, b . Then $5 = b \times a_0$, forcing $a_0 = \pm 5$, for otherwise 1 would be in N_1 . However, x is not in the ideal generated by 5, since $\langle 5 \rangle$ is the ideal of polynomials whose coefficients are all multiples of 5. Of course, there are many other examples.

Test 2 – continued

- (f) A prime ideal that is not maximal in a commutative ring with unity.

In $\mathbb{Z}[x]$, let $N_2 = \langle x \rangle$, the principal ideal generated by x . Then N_2 is prime, because if $p(x)q(x) = xr(x)$, where $p(x)$, $q(x)$ and $r(x)$ are polynomials, then either $p(x)$ or $q(x)$ must have a zero constant term, forcing $p(x)$ or $q(x)$ to be in N_2 . The ideal N_1 , defined above, is a proper ideal containing N_2 , so N_2 is not maximal.

Note: N_1 is also a prime ideal, for if $p(x)q(x) = 5k + xr(x)$, then either the constant term of $p(x)$ or the constant term of $q(x)$ is a multiple of 5, so either $q(x) \in N_1$ or $p(x) \in N_1$. Also, one can generate examples using polynomials in two "variables" or "unknowns". $\mathbb{Z}[x,y]$ can be defined directly or else as $(\mathbb{Z}[x])[y]$.

2. (a) Compute all solutions to $7x \equiv 12 \pmod{29}$. What is the largest negative solution?

SOLUTION: $\gcd(7, 29) = 1$, so a solution exists. The division algorithm gives $1 \times 29 - 4 \times 7 = 1$, so $7 \times 4 \equiv -1 \pmod{29}$. Multiply by -12 on both sides to obtain $7 \times (4)(-12) \equiv 12 \pmod{29}$. So $x = -48 \equiv -19 \equiv 10 \pmod{29}$ are solutions. -19 is the largest negative solution and 10 is the smallest positive solution. All solutions are of the form $10 + 29k$, $k \in \mathbb{Z}$.

- (b) Prove that $n^{17} - n$ is always a multiple of 17 for any integer n .

SOLUTION: 17 is a prime number, so $n^{16} = n^{17-1} = 1$ for any non-zero $n \in \mathbb{Z}_{17}$. This is equivalent to $n^{16} - 1 = 0$, for $n \neq 0$. Then $n(n^{16} - 1) = n^{17} - n = 0$ for all $n \in \mathbb{Z}_{17}$, so $n^{17} - n \equiv 0 \pmod{17}$ for any $n \in \mathbb{Z}$, so $n^{17} - n$ is always a multiple of 17.

- (c) Prove that $n^{17} - n$ is always a multiple of 510 for any integer n .

SOLUTION: Let's factor 510 to get a clue on how to proceed. $510 = 2 \times 3 \times 5 \times 17$. We already know that $n^{17} - n$ is a multiple of 17. If we can show that it is also a multiple of 2, a multiple of 3 and a multiple of 5, we are done since the least common multiple of 2, 3, 5 and 17 is 510.

If p is a prime number such that $p - 1$ divides 16, (say $16 = (p - 1)d$), then if n is not a multiple of p , $n^{p-1} \equiv 1 \pmod{p}$, so $n^{16} = (n^{p-1})^d \equiv 1^d \equiv 1 \pmod{p}$. As with 17 above, this is equivalent to $n^p - n \equiv 0 \pmod{p}$ for all $n \in \mathbb{Z}$. For the prime numbers 2, 3 and 5, note that $16 = (2 - 1) \times 16$, $16 = (3 - 1) \times 8$ and $16 = (5 - 1) \times 4$, so that $n^{17} - n$ is always a multiple of 2, 3, 5 and 17, hence a multiple of their product, 510.

Test 2 – continued

3. Dick and Jane work for the Acme Tile Company as truck drivers. Dick's truck can carry 63 tiles and Jane's truck carries 50. Dick and Jane each delivered the same number of tiles to two different customers. Dick made a certain number of trips with a full load, but carried only 20 tiles on his last trip. Similarly, Jane made a larger number of deliveries with full loads, and carried 17 tiles on her last trip. How many tiles did they each deliver, given that this number is less than four thousand?

SOLUTION: This is a classic "Chinese remainder theorem" problem. Find x , the number of tiles that both Dick and Jane delivered. x equals some number of multiples of 63 with 20 leftover tiles for a final delivery (Dick) and also equals some multiple of 50 with 17 leftover tiles for a final delivery (Jane). That is, find x such that

$$\begin{aligned} x &\equiv 20 \pmod{63}, \\ x &\equiv 17 \pmod{50}. \end{aligned}$$

63 and 50 are relatively prime. Computing their gcd leads to $50 \times 29 - 23 \times 63 = 1$. Thus, $50 \times 87 - 69 \times 63 = 3 = 20 - 17$, so $50 \times 87 + 17 = 69 \times 63 + 20$, giving a solution of 4367 tiles. All solutions to this problem are of the form $4367 + 3150k$, where k is any integer ($3150 = 63 \times 50$). The only positive solution < 4000 is $4367 - 3150 = 1217$, so they both delivered 1217 tiles. Dick made 20 deliveries (19 full loads) and Jane made 25 (24 full loads).

4. In \mathbb{Z}_3 , divide $q(x) = x^3 + x^2 + x + 2$ into $p(x) = 2x^5 - x^4 + x^3 - 2$, obtaining $p(x) = s(x) * q(x) + r(x)$. What are $s(x)$ and $r(x)$?

SOLUTION: All computations are in \mathbb{Z}_3 .

$$\begin{array}{r} 2x^2 - 1 \\ x^3 + x^2 + x + 2 \mid 2x^5 - x^4 + x^3 + 0x^2 + 0x - 2 \\ \underline{2x^5 + 2x^4 + 2x^3 + x^2} \\ -x^3 - x^2 + 0x - 2 \\ \underline{-x^3 - x^2 - x - 2} \\ x \end{array}$$

Thus, $s(x) = 2x^2 - 1$ and $r(x) = x$.

Test 2 – continued

5. In $\mathbb{Z}[x]$, is the polynomial, $15x^7 - 6x^6 + 10x^4 - 16x^3 + 2x^2 - 4x + 2$, irreducible?

SOLUTION: The prime number 2 does not divide the coefficient of the leading term, 15, but divides all the other coefficients. (They are all even.) Furthermore, $a_0 = 2$ is not a multiple of $2^2 = 4$, so the polynomial is irreducible by Eisenstein's criterion.

6. In \mathbb{Z}_p , where p is an odd prime, and a is a primitive root of unity (a generates the multiplicative group of non-zero elements), prove that $x^2 - a$ is irreducible in $\mathbb{Z}_p[x]$.

SOLUTION: $x^2 - a$ is irreducible if and only if it has a root. To obtain a contradiction, suppose that $b^2 = a$ for some $b \in \mathbb{Z}_p$. Then $b = a^m$ for some positive integer m . Hence, $a = b^2 = a^{2m}$, so $a^{2m-1} = 1$. This means that $2m - 1$, which is odd, must be a multiple of $p - 1$, which is even. This is impossible.

7. In \mathbb{Z}_{12} :

- (a) Find an irreducible polynomial (degree > 1).

SOLUTION: $x^2 + 5$. There are, of course, many other examples.

- (b) Find a monic polynomial of degree two with exactly two roots.

SOLUTION: This has to be done with some care. If the roots are a and b , then the polynomial will factor as $(x - a)(x - b)$. Then a and b must be chosen to avoid the products 2×6 and 3×4 . We may as well assume that $0 \leq a < b < 12$. We must avoid $b = a + 1$ and $b = a + 4$. A possible solution is $(x - 2)(x - 5) = x^2 - 7x + 10$.

- (c) Find a monic polynomial of degree two with more than two roots.

SOLUTION: Using the argument above, choose $a = 2$ and $b = 3$. $(x - 2)(x - 3) = x^2 - 5x + 6$ has roots 2, 3 and 6.

- (d) Find a monic polynomial of degree three with 6 roots.

SOLUTION: $(x - 1)(x - 2)(x - 5)$ has roots 1, 2, 5, 7, 10 and 11.