

1. Use the Euclidean algorithm to find $\gcd(x^8 - 1, x^6 - 1)$ in $\mathbf{Q}[x]$ and write it as a linear combination of $x^8 - 1$ and $x^6 - 1$.

Let $x^8 - 1 = f(x)$ and $x^6 - 1 = g(x)$. We have $f(x) = x^2g(x) + (x^2 - 1)$, and $g(x) = (x^4 + x^2 + 1)(x^2 - 1)$, so this shows that $\gcd(x^8 - 1, x^6 - 1) = x^2 - 1$, and $x^2 - 1 = f(x) - x^2g(x)$.

2. Are the following polynomials irreducible over \mathbf{Q} ?

(a) $3x^5 + 18x^2 + 24x + 6$

Dividing by 3 we obtain $x^5 + 6x^2 + 8x + 2$, and this satisfies Eisenstein's criterion for $p = 2$.

(b) $7x^3 + 12x^2 + 3x + 45$

Reducing the coefficients modulo 2 gives the polynomial $x^3 + x + 1$, which is irreducible in $\mathbf{Z}_2[x]$. This implies that the polynomial is irreducible over \mathbf{Q} .

(c) $2x^{10} + 25x^3 + 10x^2 - 30$

Eisenstein's criterion is satisfied for $p = 5$.

3. (a) Show that $x^2 + 1$ is irreducible over \mathbf{Z}_3 .

To show that $p(x) = x^2 + 1$ is irreducible over \mathbf{Z}_3 , we only need to check that it has no roots in \mathbf{Z}_3 , and this follows from the computations $p(0) = 1$, $p(1) = 2$, and $p(-1) = 2$.

(b) List the elements of the field $F = \mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$.

The congruence classes are in one-to-one correspondence with the linear polynomials, so we have the nine elements $[0]$, $[1]$, $[2]$, $[x]$, $[x + 1]$, $[x + 2]$, $[2x]$, $[2x + 1]$, $[2x + 2]$.

(c) In the multiplicative group of nonzero elements of F , show that $[x + 1]$ is a generator, but $[x]$ is not.

The multiplicative group of F has 8 elements, and since $[x]^2 = [-1]$, it follows that $[x]$ has order 4 and is not a generator. On the other hand, $[x + 1]^2 = [x^2 + 2x + 1] = [-1 + 2x + 1] = [2x] = [-x]$, and so $[x + 1]^4 = [-x]^2 = [-1]$, which shows that $[x + 1]$ does not have order 2 or 4. The only remaining possibility (by Lagrange's theorem) is that $[x + 1]$ has order 8, and so it is a generator for the multiplicative group of F .

4. In $\mathbf{Z}_2[x]/\langle x^3 + x + 1 \rangle$, find the multiplicative inverse of $[x + 1]$.

We first give a solution using the Euclidean algorithm. For $p(x) = x^3 + x + 1$ and $f(x) = x + 1$, the first step of the Euclidean algorithm gives $p(x) = (x^2 + x)f(x) + 1$. Thus $p(x) - (x^2 + x)f(x) = 1$, and so reducing modulo $p(x)$ gives $[-x^2 - x][f(x)] = [1]$, and thus $[x + 1]^{-1} = [-x^2 - x] = [x^2 + x]$.

We next give an alternate solution, which uses the identity $[x^3] = [x + 1]$ to solve a system of equations. We need to solve $[1] = [x + 1][ax^2 + bx + c]$ or

$$\begin{aligned} [1] &= [ax^3 + bx^2 + cx + ax^2 + bx + c] \\ &= [ax^3 + (a + b)x^2 + (b + c)x + c] \\ &= [a(x + 1) + (a + b)x^2 + (b + c)x + c] \\ &= [(a + b)x^2 + (a + b + c)x + (a + c)], \end{aligned}$$

so we need $a + b \equiv 0 \pmod{2}$, $a + b + c \equiv 0 \pmod{2}$, and $a + c \equiv 1 \pmod{2}$. This gives $c \equiv 0 \pmod{2}$, and therefore $a \equiv 1 \pmod{2}$, and then $b \equiv 1 \pmod{2}$. Again, we see that $[x + 1]^{-1} = [x^2 + x]$.

5. In $\mathbf{Z}_5[x]/\langle x^3 + x + 1 \rangle$, find $[x]^{-1}$ and $[x + 1]^{-1}$, and use your answers to find $[x^2 + x]^{-1}$.

Using the division algorithm, we obtain $x^3 + x + 1 = x(x^2 + 1) + 1$, and so $[x][x^2 + 1] = [-1]$. Thus $[x]^{-1} = [-x^2 - 1]$.

Next, we have $x^3 + x + 1 = (x + 1)(x^2 - x + 2) - 1$, and so $[x + 1]^{-1} = [x^2 - x + 2]$.

Finally, we have

$$\begin{aligned} [x^2 + x]^{-1} &= [x]^{-1}[x + 1]^{-1} = [-x^2 - 1][x^2 - x + 2] \\ &= [-x^4 + x^3 - 2x^2 - x^2 + x - 2]. \end{aligned}$$

Using the identities $[x^3] = [-x - 1]$ and $[x^4] = [-x^2 - x]$, this reduces to

$$\begin{aligned} [x^2 + x]^{-1} &= [x^2 + x - x - 1 - 3x^2 + x - 2] \\ &= [-2x^2 + x - 3] = [3x^2 + x + 2]. \end{aligned}$$

6. Let R be the ring with 8 elements consisting of all 3×3 matrices with entries in \mathbf{Z}_2 which have the following form:

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix}$$

You may assume that the standard laws for addition and multiplication of matrices are valid.

- (a) Show that R is a commutative ring (you only need to check closure and commutativity of multiplication).

It is clear that the set is closed under addition, and the following computation checks closure under multiplication.

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & c & a \end{bmatrix} \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ y & z & x \end{bmatrix} = \begin{bmatrix} ax & 0 & 0 \\ 0 & ax & 0 \\ bx + ay & cx + az & ax \end{bmatrix}$$

Because of the symmetry $a \leftrightarrow x$, $b \leftrightarrow y$, $c \leftrightarrow z$, the above computation also checks commutativity.

- (b) Find all units of R , and all nilpotent elements of R .

Four of the matrices in R have 1's on the diagonal, and these are invertible since their determinant is nonzero. Squaring each of the other four matrices gives the zero matrix, and so they are nilpotent.

- (c) Find all idempotent elements of R .

By part (b), an element in R is either a unit or nilpotent. The only unit that is idempotent is the identity matrix (in a group, the only idempotent element is the identity) and the only nilpotent element that is also idempotent is the zero matrix.

7. Let R be the ring $\mathbf{Z}_2[x]/\langle x^2 + 1 \rangle$. Show that although R has 4 elements, it is not isomorphic to either of the rings \mathbf{Z}_4 or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

In R we have $a + a = 0$, for all $a \in R$, so R is not isomorphic to \mathbf{Z}_4 . On the other hand, in R we have $[x + 1] \neq [0]$ but $[x + 1]^2 = [x^2 + 1] = [0]$. Thus R cannot be isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, since in that ring $(a, b)^2 = (0, 0)$ implies $a^2 = 0$ and $b^2 = 0$, and this implies $a = 0$ and $b = 0$ since \mathbf{Z}_2 is a field.

8. In the group \mathbf{Z}_{180}^\times of units of the ring \mathbf{Z}_{180} , what is the largest possible order of an element?

Since $180 = 2^2 \cdot 3^2 \cdot 5$, it follows from Theorem 3.5.4 that the ring \mathbf{Z}_{180} is isomorphic to the ring $\mathbf{Z}_4 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$. Then Example 5.2.10 shows that

$$\mathbf{Z}_{180}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_9^\times \times \mathbf{Z}_5^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_4.$$

In the latter additive group, the order of an element is the least common multiple of the orders of its components. It follows that the largest possible order of an element is $\text{lcm}[2, 6, 4] = 12$.

9. For the element $a = (0, 2)$ of the ring $R = \mathbf{Z}_{12} \oplus \mathbf{Z}_8$, find $\text{Ann}(a) = \{r \in R \mid ra = 0\}$. Show that $\text{Ann}(a)$ is an ideal of R .

We need to solve $(x, y)(0, 2) = (0, 0)$ for $(x, y) \in \mathbf{Z}_{12} \oplus \mathbf{Z}_8$. We only need $2y \equiv 0 \pmod{8}$, so the first component x can be any element of \mathbf{Z}_{12} , while $y = 0, 4$. Thus $\text{Ann}((0, 2)) = \mathbf{Z}_{12} \oplus 4\mathbf{Z}_8$. This set is certainly closed under addition, and it is also closed under multiplication by any element of R since $4\mathbf{Z}_8$ is an ideal of \mathbf{Z}_8 .

10. Let I be the subset of $\mathbf{Z}[x]$ consisting of all polynomials with even coefficients. Prove that I is a prime ideal; prove that I is not maximal.

Define $\phi : \mathbf{Z}[x] \rightarrow \mathbf{Z}_2[x]$ by reducing coefficients modulo 2. This is an onto ring homomorphism with kernel I . Then R/I is isomorphic to $\mathbf{Z}_2[x]$, which is not a field, so I is not maximal.

Table 1: Multiplication in $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$

\times	1	x	x^2	$x^2 + x + 1$	$x^2 + x$	$x + 1$	$x^2 + 1$
1	1	x	x^2	$x^2 + x + 1$	$x^2 + x$	$x + 1$	$x^2 + 1$
x	x	x^2	1	$x^2 + x + 1$	$x^2 + 1$	$x^2 + x$	$x + 1$
x^2	x^2	1	x	$x^2 + x + 1$	$x + 1$	$x^2 + 1$	$x^2 + x$
$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x + 1$	0	0	0
$x^2 + x$	$x^2 + x$	$x^2 + 1$	$x + 1$	0	$x^2 + x$	$x + 1$	$x^2 + 1$
$x + 1$	$x + 1$	$x^2 + x$	$x^2 + 1$	0	$x + 1$	$x^2 + 1$	$x^2 + x$
$x^2 + 1$	$x^2 + 1$	$x + 1$	$x^2 + x$	0	$x^2 + 1$	$x^2 + x$	$x + 1$

11. Let R be the ring $\mathbf{Z}_2[x]/\langle x^3 + 1 \rangle$.

Note: Table 1 gives the multiplication table.

It is not necessary to compute the multiplication table in order to solve the problem.

(a) Find all ideals of R .

By Proposition 5.3.7, the ideals of R correspond to the ideals of $\mathbf{Z}_2[x]$ that contain $\langle x^3 + 1 \rangle$. We have the factorization $x^3 + 1 = x^3 - 1 = (x - 1)(x^2 + x + 1)$, so the only proper, nonzero ideals are the principal ideals generated by $[x + 1]$ and $[x^2 + x + 1]$.

(b) Find the units of R .

We have $[x]^3 = [1]$, so $[x]$ and $[x^2]$ are units. On the other hand, $[x + 1][x^2 + x + 1] = [x^3 + 1] = [0]$, so $[x + 1]$ and $[x^2 + x + 1]$ cannot be units. This also excludes $[x^2 + x] = [x][x + 1]$ and $[x^2 + 1] = [x^2][1 + x]$. Thus the only units are 1, $[x]$, and $[x^2]$.

(c) Find the idempotent elements of R .

Using the general fact that $(a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$ (since $\mathbf{Z}_2[x]$ has characteristic 2) and the identities $[x^3] = [1]$ and $[x^4] = [x]$, it is easy to see that the idempotent elements of R are $[0]$, $[1]$, $[x^2 + x + 1]$, and $[x^2 + x]$.

12. Let S be the ring $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$.

Note: Table 2 gives the multiplication table. It is not necessary to compute the multiplication table

Table 2: Multiplication in $\mathbf{Z}_2[x]/\langle x^3 + x \rangle$

\times	1	$x^2 + x + 1$	x^2	x	$x^2 + x$	$x + 1$	$x^2 + 1$
1	1	$x^2 + x + 1$	x^2	x	$x^2 + x$	$x + 1$	$x^2 + 1$
$x^2 + x + 1$	$x^2 + x + 1$	1	x^2	x	$x^2 + x$	$x + 1$	$x^2 + 1$
x^2	x^2	x^2	x^2	x	$x^2 + x$	$x^2 + x$	0
x	x	x	x	x^2	$x^2 + x$	$x^2 + x$	0
$x^2 + x$	$x^2 + x$	$x^2 + x$	$x^2 + x$	$x^2 + x$	0	0	0
$x + 1$	$x + 1$	$x + 1$	$x^2 + x$	$x^2 + x$	0	$x^2 + 1$	$x^2 + 1$
$x^2 + 1$	$x^2 + 1$	$x^2 + 1$	0	0	0	$x^2 + 1$	$x^2 + 1$

in order to solve the problem.

(a) Find all ideals of S .

Over \mathbf{Z}_2 we have the factorization $x^3 + x = x(x^2 + 1) = x(x + 1)^2$, so by Proposition 5.3.7 the proper nonzero ideals of S are the principal ideals generated by $[x]$, $[x + 1]$, $[x^2 + 1] = [x + 1]^2$, and $[x^2 + x] = [x][x + 1]$.

$$\langle [x^2 + x] \rangle = \{[0], [x^2 + x]\} \quad \langle [x^2 + 1] \rangle = \{[0], [x^2 + 1]\}$$

$$\langle [x] \rangle = \{[0], [x], [x^2], [x^2 + x]\} \quad \langle [x + 1] \rangle = \{[0], [x + 1], [x^2 + 1], [x^2 + x]\}$$

(b) Find the units of R .

Since no unit can belong to a proper ideal, it follows from part (a) that we only need to check $[x^2+x+1]$. This is a unit since $[x^2+x+1]^2 = [1]$.

(c) Find the idempotent elements of R .

Since $[x^3] = [1]$, we have $[x^2]^2 = [x^2]$, and then $[x^2+1]^2 = [x^2+1]$. These, together with $[0]$ and $[1]$, are the only idempotents.

13. Show that the rings R and S in the two previous problems are isomorphic as abelian groups, but not as rings.

Both R and S are isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, as abelian groups. They cannot be isomorphic as rings since R has 3 units, while S has only 2.

14. Let I and J be ideals in the commutative ring R , and define the function $\phi : R \rightarrow R/I \oplus R/J$ by $\phi(r) = (r+I, r+J)$, for all $r \in R$.

(a) Show that ϕ is a ring homomorphism, with $\ker(\phi) = I \cap J$.

The fact that ϕ is a ring homomorphism follows immediately from the definitions of the operations in a direct sum and in a factor ring. Since the zero element of $R/I \oplus R/J$ is $(0+I, 0+J)$, we have $r \in \ker(\phi)$ if and only if $r \in I$ and $r \in J$, so $\ker(\phi) = I \cap J$.

(b) Show that if $I+J = R$, then ϕ is onto, and thus $R/(I \cap J) \cong R/I \oplus R/J$.

If $I+J = R$, then we can write $1 = x + y$, for some $x \in I$ and $y \in J$. Given any element $(a+I, b+J) \in R/I \oplus R/J$, consider $r = bx + ay$, noting that $a = ax + ay$ and $b = bx + by$. We have $a - r = a - bx - ay = ax - bx \in I$, and $b - r = b - bx - ay = by - ay \in J$. Thus $\phi(r) = (a+I, b+J)$, and ϕ is onto. The isomorphism follows from the fundamental homomorphism theorem.