

# Math 81: Abstract Algebra

Prishita Dharampal

**Credit Statement:** Talked to Sair Shaikh'26, and Math Stack Exchange.

**Problem 1.** For  $f(x) = x^4 - 1$  and  $g(x) = 3x^2 + 3x$  find: the quotient and remainder after dividing  $f$  by  $g$ ; the gcd of  $f$  and  $g$ ; and the expression of this gcd in the form  $af + bg$  for some  $a, b \in \mathbb{Q}[x]$ . For the last two, you'll need to recall the Euclidean Algorithm and the Bezout Identity.

*Solution.*

Quotient:  $\frac{1}{3}(x^2 - x + 1)$

Remainder:  $-x - 1$

Using Euclid's Algorithm:

$$\begin{aligned}x^4 - 1 &= (3x^2 + 3x)\left(\frac{1}{3}(x^2 - x + 1)\right) + (-x - 1) \\(3x^2 + 3x) &= (-x - 1)(-3x) + 0\end{aligned}$$

$$gcd(x^4 - 1, 3x^2 + 3x) = -x - 1$$

Using Bezout's Identity:

$$\begin{aligned}(x^4 - 1, 3x^2 + 3x) &= af + bg \\-x - 1 &= f - \left(\frac{1}{3}(x^2 - x + 1)\right)g \\-x - 1 &= 1(x^4 - 1) + \left(-\left(\frac{1}{3}(x^2 - x + 1)\right)\right)(3x^2 + 3x)\end{aligned}$$

$$a = 1, b = -\left(\frac{1}{3}(x^2 - x + 1)\right)$$

**Problem 2.** Prove that two polynomials  $f, g \in \mathbb{Z}[x]$  are relatively prime in  $\mathbb{Q}[x]$  (i.e., they share no common nonconstant factor) if and only if the ideal  $(f, g) \subset \mathbb{Z}[x]$  contains a nonzero integer.

*Solution.*

( $\implies$ )

Assume the polynomials  $f, g$  are relatively prime in  $\mathbb{Q}[x]$ .

I.e.  $(f, g) = (\gcd(f, g)) = (1) = \mathbb{Q}[x]$ . Since we are in a euclidean domain,

$$1 = af + bg$$

for some  $a, b$  with rational coefficients. Let  $k$  be the product of the denominators of the coefficients of the terms in  $a, b$ . Then

$$k = kaf + kbg$$

has integer coefficients. I.e.  $kaf, kbg \in \mathbb{Z}[x]$ , and since  $k$  can be expressed as a linear combination of  $f$  and  $g$ ,  $k \in (f, g) \subset \mathbb{Z}[x]$ . Hence, the ideal  $(f, g) \subset \mathbb{Z}[x]$  contains a nonzero integer.

( $\impliedby$ )

Assume the ideal  $(f, g) \subset \mathbb{Z}[x]$  contains a non-zero integer  $k$ .

Since this ideal is a subset of the ideal generated by  $f, g$  in  $\mathbb{Q}[x]$ ,  $k \in (f, g) \subset \mathbb{Q}[x]$ . But all integers are units in  $\mathbb{Q}[x] \implies 1 \in (f, g) \subset \mathbb{Q}[x]$ . I.e. for some polynomials  $a, b \in \mathbb{Q}[x]$ ,

$$1 = af + bg$$

Hence, the polynomials  $f, g$  are relatively prime in  $\mathbb{Q}[x]$ .

**Problem 3.** Decide whether each of the following polynomials is irreducible, and if not, then find the factorization into monic irreducibles.

1.  $x^4 + 1 \in \mathbb{R}[x]$
2.  $x^4 + 1 \in \mathbb{Q}[x]$
3.  $x^7 + 66x^6 - 77x + 737 \in \mathbb{Q}[x]$
4.  $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$
5.  $x^3 + 5x^2 - 9x + 3 \in \mathbb{Q}[x]$

*Solution.*

1.  $x^4 + 1 \in \mathbb{R}[x]$   

$$(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

2.  $x^4 + 1 \in \mathbb{Q}[x]$  Let  $f(x) = x^4 + 1$ . Then,

$$f(y+1) = (y+1)^4 + 1 = y^4 + 4y^3 + 6y^2 + 4y + 2$$

We can see that  $2|4$ ,  $2|6$ ,  $2|2$ , and  $4 \nmid 2$ . Then by Eisentein's Criterion, the polynomials of the form  $f(x)$  are irreducible in  $\mathbb{Q}[x]$ .

3.  $x^7 + 66x^6 - 77x + 737 \in \mathbb{Q}[x]$

We can see that  $11|66$ ,  $11| - 77$ ,  $11|737$ , and  $121 \nmid 737$ . Then by Eisentein's Criterion, the polynomial is irreducible in  $\mathbb{Q}[x]$ .

4.  $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$

Let  $f(x) = x^4 + x^3 + x^2 + x + 1$ . Then,

$$f(y+1) = (y+1)^4 + (y+1)^3 + (y+1)^2 + 1 = y^4 + 5y^3 + 10y^2 + 10y + 5$$

We can see that  $5|5$ ,  $5|10$ , and  $25 \nmid 5$ . Then by Eisentein's Criterion, the polynomials of the form  $f(x)$  are irreducible in  $\mathbb{Q}[x]$ .

5.  $x^3 + 5x^2 - 9x + 3 \in \mathbb{Q}[x]$

Assume  $\frac{r}{s}$  is a root of the polynomial in the lowest terms. From proposition 11 we know that  $r|a_n$  and  $s|a_0$ . I.e.  $r|1$ ,  $s|3$ . The only such candidate is  $\frac{1}{3}$ . Checking,

$$\left(\frac{1}{3}\right)^3 + 5\left(\frac{1}{3}\right)^2 - 9\left(\frac{1}{3}\right) + 3 = \frac{16}{27}$$

Hence,  $\frac{16}{27}$  is not a root of the polynomial. By proposition 10, we know that this polynomial (degree 3) is irreducible in  $\mathbb{Q}[x]$  (over a field).

**Problem 4.** *Irreducible polynomials over finite fields.* Let  $\mathbb{F}_3$  be the field with three elements.

1. Determine all the monic irreducible polynomials of degree  $\leq 3$  in  $\mathbb{F}_3[x]$ .
2. Determine the number of monic irreducible polynomials of degree 4 in  $\mathbb{F}_3[x]$ .

**Hint.** This is easier than determining all of them.

*Solution.*

1. (a) Linear Irreducible Polynomials

By definition all monic linear polynomials are irreducible.

$$\begin{aligned}x &= 0 \\x + 1 &= 0 \\x + 2 &= 0\end{aligned}$$

- (b) Quadratic Irreducible Polynomials

All quadratic polynomials are of the form  $x^2 + ax + b = 0$ , where  $a, b \in \mathbb{F}_3$ . There are 9 such polynomials. By Proposition 10, we know that polynomials of degree two over a field is reducible if and only if it has a root in the field.

Upon checking, we are left with:

$$\begin{aligned}x^2 + 1 &= 0 \\x^2 + 1x + 2 &= 0 \\x^2 + 2x + 2 &= 0\end{aligned}$$

- (c) Cubic Irreducible Polynomials All cubic polynomials are of the form  $x^3 + ax^2 + bx + c = 0$ , where  $a, b, c \in \mathbb{F}_3$ . There are 27 such polynomials. By Proposition 10, we know that polynomials of degree three over a field is reducible if and only if it has a root in the field.

Upon checking, we are left with:

$$\begin{aligned}
 x^3 + 2x + 1 &= 0 \\
 x^3 + 2x + 2 &= 0 \\
 x^3 + 1x^2 + 2 &= 0 \\
 x^3 + 1x^2 + 2x + 1 &= 0 \\
 x^3 + 1x^2 + 1x + 2 &= 0 \\
 x^3 + 2x^2 + 1 &= 0 \\
 x^3 + 2x^2 + 1x + 1 &= 0 \\
 x^3 + 2x^2 + 2x + 2 &= 0
 \end{aligned}$$

## 2. Quartic Irreducible Polynomials

All cubic polynomials are of the form  $x^4 + ax^3 + bx^2 + cx + d = 0$ , where  $a, b, c, d \in \mathbb{F}_3$ . There are 81 such polynomials. To the irreducibles we first count the reducibles. The reducibles can be classified by the degrees of their factors that is partitions of 4.

- $3 + 1$

There are 8 irreducible cubics and 3 irreducible linear polynomials, the number of quartics factored as such are:  $8 \cdot 3 = 24$ .

- $2 + 2$

There are 3 irreducible quadratics, the number of quartics factored as such are:  $3! = 6$

- $2 + 1 + 1$

There are 3 irreducible quadratics, and 3 irreducible linear polynomials, the number of quartics factored as such are:  $3 \cdot (3!) = 18$ .

- $1 + 1 + 1 + 1$

There are 3 irreducible linear polynomials and 4 places to fill, so by stars and bars

the number of quartics that can be factored as such are:  $\binom{6}{2} = 15$ .

Then the number of irreducible quartics is

$$81 - 24 - 6 - 18 - 15 = 18.$$

**Problem 5(a).** *Symmetric polynomials.* Let  $R$  be a commutative ring with 1 and  $R[x_1, \dots, x_n]$  the ring of polynomials in the variables  $x_1, \dots, x_n$  with coefficients in  $R$ . Consider the symmetric group  $S_n$  acting on the set  $\{x_1, \dots, x_n\}$  by permutations. Extend this action linearly to  $R[x_1, x_2, \dots, x_n]$ ; for example, if  $\sigma = (123) \in S_3$ , then

$$\sigma \cdot (x_1x_2 - 6x_3^2 + 7x_2x_3^2) = x_2x_3 - 6x_1^2 + 7x_3x_1^2.$$

Then this action satisfies  $\sigma \cdot (f + g) = \sigma \cdot f + \sigma \cdot g$  and  $\sigma \cdot (fg) = (\sigma \cdot f)(\sigma \cdot g)$  for all  $\sigma \in S_n$  and all  $f, g \in R[x_1, \dots, x_n]$ .

Let  $S \subset R[x_1, \dots, x_n]$  be the subset fixed under the action of  $S_n$ . Prove that  $S$  is a subring with 1. This is called the **ring of symmetric polynomials**.

*Solution.*

To prove that  $S$  is a subring with 1:

1. Contains 1

Since 1 is a constant polynomial and  $S_n$  is acting on the set of variables  $\{x_1, \dots, x_n\}$ ,

$$\sigma(1) = 1$$

Hence,  $1 \in S$ .

2. Closed under multiplication

$\forall f, g \in S$  by definition,  $\sigma(f) = f, \sigma(g) = g$  and again by definition,

$$\sigma(fg) = \sigma(f) \cdot \sigma(g) = f \cdot g$$

Hence,  $f \cdot g \in S$ . Since  $f, g$  were arbitrary polynomials this holds for any elements in  $S$  and  $S$  is closed under multiplication.

**Problem 5(b).** For each  $n \geq 0$ , define polynomials  $e_i \in R[x_1, \dots, x_n]$  by  $e_0 = 1$  and

$$e_1 = x_1 + \dots + x_n, \quad e_2 = \sum_{1 \leq i < j \leq n} x_i x_j, \quad \dots, \quad e_n = x_1 \cdots x_n$$

and  $e_k = 0$  for  $k > n$ . In words,  $e_k$  is the sum of all distinct products of subsets of  $k$  distinct variables. Prove that each  $e_k$  is a symmetric polynomial. These are called the **elementary symmetric polynomials**.

*Solution.*

For a given  $k$ ,  $1 \leq k \leq n$ ,

$$e_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

Let  $A$  be the set of all terms in  $e_k$ .

$$A = \{x_{i_1} x_{i_2} \cdots x_{i_k} \mid 1 \leq i_1 < i_2 < \dots < i_k \leq n\}$$

Since  $\sigma$  as a  $n$ -cycle is a bijection on  $\{i_1, i_2, \dots, i_n\}$ ,  $\forall a \in A$ ,  $\sigma(a)$  is also a product of  $k$  distinct variables. And by definition of  $A$  all distinct multiples of subsets of  $k$  distinct variables,  $\sigma(a) \in A$ . Hence,  $\sigma : A \rightarrow A$ .

Also, for any  $a \in A$  we can find  $b \in A$  such that  $\sigma^{-1}(b) = a$ . Hence  $\sigma$  is surjective. A surjective mapping from  $A$  to  $A$  is bijective.

Hence,  $\sigma(e_k)$  only permutes the terms of  $e_k$ .

$$\sigma(e_k) = \sum_{a \in A} \sigma(a) = \sum_{a \in A} a = e_k$$

$e_k$  is invariant under the action of  $\sigma$ , and hence is a symmetric polynomial.

**Problem 5(c).** The **generic polynomial** of degree  $n$  is the polynomial

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

in the ring  $R[x_1, \dots, x_n][x]$  of polynomials in  $x$  with coefficients in  $R[x_1, \dots, x_n]$ . Prove (by induction) that

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \cdots + (-1)^n e_n \\ &= \sum_{j=0}^n (-1)^{n-j} e_{n-j} x^j. \end{aligned}$$

*Solution.*

**Base case:**  $n = 1, R[x_1][x]$

Then, by definition,

$$f(x) = x - x_1$$

In  $R[x_1][x]$ ,  $e_1$  is the sum of all distinct products of subsets of 1 distinct variables. I.e.  $e_1 = x_1$ . Upon substitution.

$$\begin{aligned} f(x) &= x - x_1 \\ &= x - e_1 \\ &= x + (-1)^1 e_1 \\ &= (-1)^0 e_0 x + (-1)^1 e_1 x^0 \\ &= (-1)^1 e_1 x^0 + (-1)^0 e_0 x \\ &= \sum_{j=0}^1 (-1)^{1-j} e_{1-j} x^j \end{aligned}$$

Hence, base case holds.

**Notation:**  $e_{a,k}$ , where  $a$  refers to the elementary symmetric polynomials in  $R[x_1, \dots, x_a][x]$ , or in a ring with  $a$  adjoined variables, and  $k$  refers to the number of variables in the subset. For example, in  $R[x_1 \cdots x_n][x]$ , the elementary symmetric polynomial with  $j$  elements in the subset as  $e_{n,j}$ .

**Inductive Hypothesis:** Assume the  $n - 1$  the case holds. I.e. in  $R[x_1, \dots, x_{n-1}][x]$ ,

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2) \cdots (x - x_{n-1}) = x^{n-1} - e_1 x^{n-2} + e_2 x^{n-3} + \cdots + (-1)^{n-1} e_{n-1} \\ &= \sum_{j=0}^{n-1} (-1)^{n-1-j} e_{(n-1), (n-1-j)} x^j \end{aligned}$$

**Inductive Step:**  $n = n, R[x_1, \dots, x_n][x]$

Then, by definition,

$$f'(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

Upon substitution,

$$\begin{aligned} f'(x) &= (x - x_1)(x - x_2) \cdots (x - x_n) \\ f'(x) &= f(x)(x - x_n) \quad \text{where } f(x) \text{ is from IH} \\ &= \left( \sum_{j=0}^{n-1} (-1)^{n-1-j} e_{(n-1), (n-1-j)} x^j \right) (x - x_n) \\ &= x \left( \sum_{j=0}^{n-1} (-1)^{n-1-j} e_{(n-1), (n-1-j)} x^j \right) - x_n \left( \sum_{j=0}^{n-1} (-1)^{n-1-j} e_{(n-1), (n-1-j)} x^j \right) \end{aligned}$$

(Reindexing j)

$$\begin{aligned} &= \left( x^n + \sum_{j=0}^{n-1} (-1)^{n-j} e_{(n-1), (n-j)} x^j \right) - \left( \sum_{j=0}^{n-1} (-1)^{n-1-j} x_n e_{(n-1), (n-1-j)} x^j \right) \\ &= x^n + \sum_{j=0}^{n-1} x^j \left( (-1)^{n-j} e_{(n-1), (n-j)} + (-1)^{n-j} x_n e_{(n-1), (n-1-j)} \right) \\ &= \left( x^n + \sum_{j=0}^{n-1} x^j (-1)^{n-j} (e_{(n-1), (n-j)} + x_n e_{(n-1), (n-1-j)}) \right) \end{aligned}$$

$x_n e_{(n-1), (n-1-j)}$  represents all the elements in  $e_{n, (n-1-j)}$  that contain  $x_n$  as  $e_{(n-1), (n-1-j)}$  contains all combinations of terms from  $x_1, \dots, x_{n-1}$ . And  $e_{(n-1), (n-1-j)}$  all elements in  $e_{n, (n-1-j)}$  that don't. So, their sum equals  $e_{(n), (n-j)}$ . Overall this gives,

$$\begin{aligned} f'(x) &= \left( x^n + \sum_{j=0}^{n-1} x^j (-1)^{n-j} e_{(n), (n-j)} \right) \\ &= \left( \sum_{j=0}^n x^j (-1)^{n-j} e_{(n), (n-j)} \right) \end{aligned}$$

where the last equation follows as  $(-1)^{n-n} e_{(n), n-n} = 1$ .

**Problem 5(d).** For each  $k \geq 1$ , define the **power sums**  $p_k = x_1^k + \cdots + x_n^k$  in  $R[x_1, \dots, x_n]$ . Clearly, the power sums are symmetric. Verify the following identities by hand:

$$p_1 = e_1, \quad p_2 = e_1 p_1 - 2e_2, \quad p_3 = e_1 p_2 - e_2 p_1 + 3e_3$$

In general **Newton's identities** in  $R[x_1, \dots, x_n]$  are (recall that  $e_k = 0$  for  $k > n$ ):

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} - \cdots + (-1)^{k-1} e_{k-1} p_1 + (-1)^k k e_k = 0.$$

Prove Newton's identities whenever  $k \geq n$ .

**Hint.** For each  $i$ , consider the equation in part (c) for  $f(x_i)$  and sum all these equations together. This gives Newton's identity for  $k = n$ . Set extra variables to zero to get the identities for  $k > n$  from this. (Fun. Can you come up with a proof when  $1 \leq k \leq n$ ?)

*Solution.*

$$1. \quad p_1 = e_1$$

$$p_1 = x_1^1 + \cdots + x_n^1 = e_1$$

$$2. \quad p_2 = e_1 p_1 - 2e_2$$

$$\begin{aligned} e_1 p_1 - 2e_2 &= e_1^2 - 2e_2 \\ &= (x_1 + \cdots + x_n)^2 - 2 \left( \sum_{1 \leq i < j \leq n} x_i x_j \right) \\ &= \left( x_1^2 + \cdots + x_n^2 + 2 \left( \sum_{1 \leq i < j \leq n} x_i x_j \right) \right) - \left( \sum_{1 \leq i < j \leq n} x_i x_j \right) \\ &= x_1^2 + \cdots + x_n^2 \\ &= p_2 \end{aligned}$$

$$3. \quad p_3 = e_1 p_2 - e_2 p_1 + 3e_3$$

$$\begin{aligned}
e_1 p_2 &= \sum_{1 \leq i, j \leq n} x_i x_j^2 \\
&= \sum_{1 \leq i, j \leq n, i=j} x_i^3 + \sum_{1 \leq i < j \leq n} x_i x_j^2 + \sum_{1 \leq j < i \leq n} x_i x_j^2 \\
&= \sum_{1 \leq i, j \leq n, i=j} x_i^3 + \sum_{1 \leq i < j \leq n} x_i x_j^2 + \sum_{1 \leq i < j \leq n} x_i^2 x_j \\
e_2 p_1 &= \sum_{\substack{1 \leq i < j \leq n \\ 1 \leq k \leq n}} x_i x_j x_k \\
&\quad (\text{Using cases: } j < i < k, i < k < j, i < k < j, k = i, k = j) \\
&= \sum_{1 \leq k < i < j \leq n} x_i x_j x_k + \sum_{1 \leq i < k < j \leq n} x_i x_j x_k + \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i < j \leq n} x_i^2 x_j + \sum_{1 \leq i < j \leq n} x_i x_j^2 \\
&\quad (\text{After re-indexing, we get:}) \\
&= 3 \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i < j \leq n} x_i^2 x_j + \sum_{1 \leq i < j \leq n} x_i x_j^2 \\
e_3 &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k
\end{aligned}$$

Substituting values in,

$$\begin{aligned}
e_1 p_2 - e_2 p_1 + 3e_3 &= \sum_{1 \leq i, j \leq n, i=j} x_i^3 + \sum_{1 \leq i < j \leq n} x_i x_j^2 + \sum_{1 \leq i < j \leq n} x_i^2 x_j \\
&\quad - \left( 3 \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i < j \leq n} x_i^2 x_j + \sum_{1 \leq i < j \leq n} x_i x_j^2 \right) + 3 \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \\
&= \sum_{1 \leq i, j \leq n, i=j} x_i^3 \\
&= p_3
\end{aligned}$$

4. Newton's identities for  $k \geq n$ .

Let  $f = (x - x_1) \cdots (x - x_n)$ . For each  $x_i$ ,  $(x - x_i)$  is a factor of  $f$ . Thus,  $f(x_i) = 0$  for

all  $i$ . Summing these from 1 to  $n$  and using part (c) we get,

$$\begin{aligned}
0 &= \sum_{i=1}^n f(x_i) \\
&= \sum_{i=1}^n \left( \sum_{j=0}^n (-1)^{n-j} e_{n-j} x^j \right) \\
&= \sum_{i=1}^n (x_i^n - e_1 x_i^{n-1} + e_2 x^{n-1} + \cdots + e_{n-1} x (-1)^n e_n) \\
&= \sum_{i=1}^n x_i^n - \sum_{i=1}^n e_1 x_i^{n-1} + \sum_{i=1}^n e_2 x_i^{n-2} + \cdots + (-1)^{n-1} \sum_{i=1}^n e_{n-1} x_i + (-1)^n e_n \\
&= \sum_{i=1}^n x_i^n - e_1 \sum_{i=1}^n x_i^{n-1} + e_2 \sum_{i=1}^n x_i^{n-2} + \cdots + (-1)^{n-1} e_{n-1} \sum_{i=1}^n x_i + (-1)^n e_n \\
&= p_n - e_1 p_{n-1} + e_2 p_{n-2} + \cdots + (-1)^{n-1} e_{n-1} p_1 + (-1)^n e_n
\end{aligned}$$

Consider the ring  $R[x_1, \dots, x_n, \dots, x_k]$ . Here the equation,

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} + \cdots + (-1)^{k-n} e_n p_{k-n} + \cdots + (-1)^{k-1} e_{k-1} p_1 + (-1)^k e_k = 0$$

holds. Since,  $\forall i > n, e_i = 0$ ,

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} + \cdots + (-1)^{k-n} e_n p_{k-n} = 0$$

**Problem 6.** Use the force, my Newton!

1. If  $x, y, z$  are complex numbers satisfying

$$x + y + z = 1, \quad x^2 + y^2 + z^2 = 6, \quad x^3 + y^3 + z^3 = 7,$$

then prove that  $x^n + y^n + z^n$  is rational for any positive integer  $n$ .

2. Calculate  $x^4 + y^4 + z^4$ .
3. Prove that each of  $x, y, z$  are not rational numbers.

*Solution.*

1. Base Case: for  $n = 1, 2, 3$  we know that  $x^n + y^n + z^n$  is rational.

Induction Hypothesis: Assume  $x^k + y^k + z^k$  is rational,  $\forall k < n$ .

Inductive Step: For  $n$ , as  $n > 3$ , the following holds (from 5(d)), also  $e_i = 0, \forall i > 3$ :

$$p_n - e_1 p_{n-1} + e_2 p_{n-2} - e_3 p_{n-3} = 0$$

And,

$$p_n = e_1 p_{n-1} - e_2 p_{n-2} + e_3 p_{n-3}$$

In  $R[x, y, z]$ ,  $p_n := x^n + y^n + z^n$ .

Note:  $e_1 = p_1, e_2 = (e_1 p_1 - p_2)/2, e_3 = (p_3 - e_1 p_2 + e_2 p_1)/3, e_4 = 0$  as  $4 > 3$ .

So,  $e_1 = 1, e_2 = -5/2, e_3 = -1/2, e_4 = 0$ , which are all rational. And since,  $p_{n-1}, p_{n-2}, p_{n-3}$  are also rational (by IH) we have a sum of products of rationals, which is rational as  $\mathbb{Q}$  is a field.

2. In  $R[x, y, z]$ ,  $p_n := x^n + y^n + z^n$

$$\begin{aligned} 0 &= p_4 - e_1 p_3 + e_2 p_2 + (-1)^3 e_3 p_1 + (-1)^4 e_4 \\ &= p_4 - e_1(7) + e_2(6) - e_3(1) + e_4 \\ p_4 &= e_1 7 - e_2(6) + e_3(1) - e_4 \end{aligned}$$

Note:  $e_1 = p_1, e_2 = (e_1 p_1 - p_2)/2, e_3 = (p_3 - e_1 p_2 + e_2 p_1)/3, e_4 = 0$  as  $4 > 3$ .

So, we get  $e_1 = 1, e_2 = -5/2, e_3 = -1/2, e_4 = 0$ .

Substituting the values:

$$\begin{aligned} p_4 &= 7 - (-5/2)(6) + (-1/2) - 0 \\ &= 7 + 15 - 1/2 \\ &= 21.5 = 43/2 \end{aligned}$$

3. Let  $f(a) = (a - x)(a - y)(a - z)$  in  $\mathbb{Q}[n]$ .

$$\begin{aligned} f(a) &= a^3 - a^2(x + y + z) + a(xy + yz + zx) - xyz \\ &= a^3 - a^2(e_1) + a(e_2) - e_3 \\ &= a^3 - a^2 - (5/2)a + 1/2 \end{aligned}$$

If  $2f(a)$  has a root, then  $f(a)$  also has the same root. Rationalizing denominators,

$$2f(a) = 2a^3 - 5a + 1$$

By rational root test, any root of  $2f(a)$ , say  $\left(\frac{p}{q}\right)$  must be such that  $p|2$  and  $q|1$ . Since two is prime, there is only one root we need to check, namely  $\left(\frac{p}{q}\right) = 2$ . Checking,

$$2f(2) = 2(2)^3 - 5(2) + 1 = 16 - 10 + 1 = 7 \neq 0$$

Hence, 2 is not a root,  $f(a)$  doesn't have any rational roots and  $x, y, z$  must be irrational.