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.

Quotinent: $\frac{1}{3}(x^2 - x + 1)$
Remainder: $-x - 1$
Using Euclid's Algorithm:

$$x^4 - 1 = (3x^2 + 3x)(\frac{1}{3}(x^2 - x + 1)) + (-x - 1)$$
$$(3x^2 + 3x) = (-x - 1)(-3x) + 0$$

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

Using Bezout's Idenity:

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

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

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 $f(x) = x^4 + x^3 + x^2 + 1$. 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 $r \mid a_n$ and $s \mid a_0$. I.e. $r \mid 1$, $s \mid 3$. 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 ≤ 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.

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

$$\sigma \cdot (x_1 x_2 - 6x_3^2 + 7x_2 x_3^2) = x_2 x_3 - 6x_1^2 + 7x_3 x_1^2.$$

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 $f, g \in R[x_1, \ldots, x_n]$.
Let $S \subset R[x_1, \ldots, x_n]$ 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**.

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

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

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**.

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

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

Problem 5(d). For each $k \geq 1$, define the **power sums** $p_k = x_1^k + \cdots + x_n^k$ in $R[x_1, \ldots, x_n]$. 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 $R[x_1, \ldots, x_n]$ 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 $1 \leq k \leq n$?)

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

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

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

   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.