Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2019

Problem Set # 1 (due in class on Thursday 24 January)

Notation: If R is a commutative ring with 1, denote by $R[x_1, \dots, x_n]$ the ring of polynomials in the variables $x_1, \dots, x_n$ with coefficients in R.

Reading: FT 1, pp. 6–12.

Problems:

1. For each of the following pairs of polynomials $f, g \in \mathbb{Q}[x]$ 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 $a, b \in \mathbb{Q}[x]$.

(a) $f(x) = x^4 - 1$, $g(x) = x^2 + 1$

(b) $f(x) = x^4 - 1$, $g(x) = 3x^2 + 3x$

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

(a) $x^4 + 1 \in \mathbb{R}[x]$

(b) $x^4 + 1 \in \mathbb{Q}[x]$

(c) $x^7 + 11x^3 - 33x + 22 \in \mathbb{Q}[x]$

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

(e) $x^3 - 7x^2 + 3x + 3 \in \mathbb{Q}[x]$

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

(a) Determine all the monic irreducible polynomials of degree ≤ 3 in $\mathbb{F}_3[x]$.

(b) Determine the number of monic irreducible polynomials of degree 4 in $\mathbb{F}_3[x]$.

4. 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.

5. Let F be a field and $x_1, \dots, x_n$ be variables. Consider the **Vandermonde matrix**

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

(a) Prove that $\det(V) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$. You can do row and column reduction and use the multilinear properties of the determinant in order to set up a proof by induction.

(b) Assume that $n < |F|$, in particular, any n is allowed if F is infinite. Prove that if a polynomial $f(x) \in F[x]$ of degree n satisfies $f(a) = 0$ for all $a \in F$, then $f(x)$ is the zero polynomial. In conclusion, show that if F is infinite, the evaluation homomorphism $F[x] \to \mathrm{Map}(F, F)$, defined by $f \mapsto (a \mapsto f(a))$, is injective.

(c) Show that if $F = \mathbb{F}_p$, then $f(x) = x^p - x$ has every field element as a root. In this case, prove that $x^p - x$ generates the whole kernel of the evaluation homomorphism.

6. *Symmetric polynomials.* Let R be a commutative ring with 1 and $x_1, \dots, x_n$ be variables.

(a) Consider the symmetric group S_n acting on the set $\{x_1, \dots, x_n\}$ by permutations. Extend this action to $R[x_1, x_2, \dots, x_n]$. For example, if $\sigma = (123) \in S_3$, then

$$\sigma \cdot (x_1x_2 - 2x_3^2 + 3x_2x_3^2) = x_2x_3 - 2x_1^2 + 3x_3x_1^2.$$

Prove that 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 $f, g \in R[x_1, \dots, x_n]$. Hint. Consider monomials.

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

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

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

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**.

(d) 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

$$f(x) = (x-x_1)(x-x_2)\cdots(x-x_n) = x^n - e_1x^{n-1} + e_2x^{n-2} + \cdots + (-1)^n e_n = \sum_{j=0}^{n} (-1)^{n-j} e_{n-j} x^j.$$

(e) 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:

$$p_1 = e_1, \quad p_2 = e_1p_1 - 2e_2, \quad p_3 = e_1p_2 - e_2p_1 + 3e_3$$

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

$$p_k - e_1p_{k-1} + e_2p_{k-2} - \cdots + (-1)^{k-1}e_{k-1}p_1 + (-1)^k k e_k = 0.$$

Prove Newton's identities whenever $k \geq n$.
Hint. For each i, consider the equation in part (d) 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 $1 \leq k \leq n$?)

7. *Use the force, my Newton!*

(a) If x, y, z are complex numbers satisfying

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

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

(b) Calculate $x^4 + y^4 + z^4$.

(c) Prove that each of x, y, z are not rational numbers.

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: `asher.auel@yale.edu`