MOP 2018: FIELDS AND FROBENIUS (06/05, K)

VICTOR WANG

1. Polynomials and fields

Let K be your favorite field, like $\mathbb{Q}$ or $\mathbb{Q}[i]$ or $\mathbb{Q}(\zeta_{257})$ or $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{F}_p$.

Definition 1.1 (Non-zero polynomial, polynomial identity, irreducible polynomial)**.** As an example of multiplication, $(x+1)(x+2)(x+3) = x^3+x^2+x+1$ in $\mathbb{F}_5[x]$.

Definition 1.2 (Field extensions, finite, algebraic vs. transcendental, degree)**.**

Problem 1.3. A finite (finite-dimensional) field extension L/K is algebraic.

Problem 1.4. The sum and product of two algebraic elements over K is still algebraic. The reciprocal of any nonzero algebraic element is algebraic.

Problem 1.5. If $\alpha \in L/K$ is algebraic, then $K[\alpha] = K(\alpha)$.

Problem 1.6 (Degree is multiplicative in towers)**.** If L/K and M/L are finite field extensions, then $[M:K] = [M:L]\cdot[L:K]$.

Question 1.7. How are field *extensions* L/K related to *roots* of polynomials in $K[x]$?

Definition 1.8 (Algebraist's dream: the quotient construction)**.**

Definition 1.9 (Be the change unseen in the world: algebraic closure, conjugates)**.**

Problem 1.10. Let L/K be a field extension. Then an element $\alpha \in L$ lies in K, the base field, if and only if $\deg_K \alpha = 1$. If $K = \mathbb{F}_p$, this happens if and only if $\alpha^p = \alpha$.

Problem 1.11. Let $p_1, \ldots, p_n$ be distinct primes. Prove that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

Problem 1.12 (Characteristic)**.** A field F either contains $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p.[1]

Theorem 1.13 (Primitive element theorem)**.** *If L/K is finite and K contains $\mathbb{Q}$, then $L = K(\beta)$ for some element $\beta \in L$ (not unique).*

2. Characteristic p and the Frobenius map

Problem 2.1. Let A be a (commutative) ring such that $pa = 0$ for all $a \in A$. Then A is a $\mathbb{F}_p$-vector space, and the function $\mathrm{Fr}_p\colon A \to A, a \mapsto a^p$, is $\mathbb{F}_p$-*linear*. Write this out explicitly.

The linear map Fr_p is called the pth-power *Frobenius map*. The qth-power map $\mathrm{Fr}_q = \mathrm{Fr}_p^r$ is also $\mathbb{F}_p$-linear for prime powers $q = p^r$.

[1] To do this problem, think about the smallest positive integer n such that $n = 0$, if it exists.

Problem 2.2 (Mark Sellke, USA Dec TST for IMO 2016)**.** Define $\Psi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ by

$$\Psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i x^{p^i}.$$

Prove that for nonzero[2] polynomials $F, G \in \mathbb{F}_p[x]$,

$$\Psi(\gcd(F,G)) = \gcd(\Psi(F), \Psi(G)),$$

where the gcd is defined to be the greatest common *monic* factor (leading coefficient 1).

3. Finite fields

Problem 3.1. A *finite field* (field of finite size) must have size $q = p^r$, a prime power.

For $\mathbb{Z}/p^n$, the integers mod p^n, don't form a field if $n \geq 2$. But still, there is a field of size exactly p^n, which is unique in some sense (up to isomorphism[3]). One proof is as follows.

Problem 3.2 (Existence++)**.** Let f be a *monic* irreducible degree $d \geq 1$ polynomial in $\mathbb{F}_p[x]$.

(1) Show that $f(x) \mid g(x)^{p^d} - g(x)$ in $\mathbb{F}_p[x]$ for any $g \in \mathbb{F}_p[x]$.[4]
(2) Show that $x^{p^r} - x \mid g(x)^{p^r} - g(x)$ for any $g \in \mathbb{F}_p[x]$ and positive integer r.
(3) For positive integers r, show that $f(x) \mid x^{p^r} - x$ modulo p if and only if $d \mid r$.
(4) Let $L = \mathbb{F}_p[x]/(f(x))$, and let $\overline{x}$ represent $x \pmod{f(x)}$. Show that $f(T) = \prod_{k=0}^{d-1}(T - \overline{x}^{p^k})$ in $L[T]$.

Problem 3.3 (Uniqueness)**.** Let L/K be a field extension, where the base field K is a finite field of order $q = p^r$. Then an element $\alpha \in L$ lies in K if and only if $\alpha^q = \alpha$.

The unique field of size q is called $\mathbb{F}_q$.

Problem 3.4. When does $\mathbb{F}_{p^m}$ contain $\mathbb{F}_{p^n}$? When it does, what is the *degree* of the extension? When is $\mathrm{Fr}_{p^m} : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ an $\mathbb{F}_{p^n}$-linear map?

This is only one of many approaches to introducing finite fields. Other common routes:

- Consider the splitting field of $x^q - x$ (basically [up to isomorphism] the smallest field where it fully factors, and we can use our intuition from complex polynomials and FTA), which behaves nicely by Frobenius. (In the approach above Frobenius doesn't have as central a role.)
- *Define* $\mathbb{F}_q$ as the solution set to $x^q = x$ in the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

Finite fields appear in many places, from computer science to combinatorics to Galois theory, number theory, and algebraic geometry. But for now, here's some more theory:

Theorem 3.5 (Existence of primitive roots in finite fields)**.** $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$*, the set of nonzero elements of* $\mathbb{F}_q$*, forms a cyclic group of order* $q-1$*.*

Problem 3.6. The *norm* $\mathrm{Nm} := \prod_{j=0}^{d-1} \mathrm{Fr}_q^j$ maps $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$. It is multiplicative and surjective.

Problem 3.7. The *trace* $\mathrm{Tr} := \sum_{j=0}^{d-1} \mathrm{Fr}_q^j$ maps $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$. It is $\mathbb{F}_q$-linear and surjective.

[2] A non-zero polynomial is a polynomial with not all coefficients 0.

[3] However, there may be more than one isomorphism between two finite fields of the same size. This point of *ambiguity* is addressed by the *Galois theory* (theory of algebraic symmetries) of finite fields.

[4] If $d = 1$, this is just Fermat's little theorem: do you see why?