MOP 2018: ALGEBRAIC CONJUGATES AND NUMBER THEORY (06/15, BK)

VICTOR WANG

1. Arithmetic properties of polynomials

Problem 1.1. If $P, Q \in \mathbb{Z}[x]$ share no (complex) roots, show that there exists a finite set of primes S such that $p \nmid \gcd(P(n), Q(n))$ holds for all primes $p \notin S$ and integers $n \in \mathbb{Z}$.

Problem 1.2. If $P, Q \in \mathbb{C}[t, x]$ share no common factors, show that there exists a finite set $S \subset \mathbb{C}$ such that $(P(t, z), Q(t, z)) \neq (0, 0)$ holds for all complex numbers $t \notin S$ and $z \in \mathbb{C}$.

Problem 1.3 (USA TST 2010/1)**.** Let $P \in \mathbb{Z}[x]$ be such that $P(0) = 0$ and

$$\gcd(P(0), P(1), P(2), \dots) = 1.$$

Show there are infinitely many n such that

$$\gcd(P(n) - P(0), P(n + 1) - P(1), P(n + 2) - P(2), \dots) = n.$$

Problem 1.4 (Calvin Deng)**.** Is $\mathbb{R}[x]/(x^2 + 1)^2$ isomorphic to $\mathbb{C}[y]/y^2$ as an $\mathbb{R}$-algebra?

Problem 1.5 (ELMO 2013, Andre Arslan, one-dimensional version)**.** For what polynomials $P \in \mathbb{Z}[x]$ can a positive integer be assigned to every integer so that for every integer $n \geq 1$, the sum of the n^1 integers assigned to any n consecutive integers is divisible by $P(n)$?

2. Algebraic conjugates and symmetry

2.1. General theory.

Let $\overline{\mathbb{Q}}$ denote the set of *algebraic numbers* (over $\mathbb{Q}$), i.e. roots of polynomials in $\mathbb{Q}[x]$.

Proposition-Definition 2.1. *If $\alpha \in \overline{\mathbb{Q}}$, then there is a unique monic polynomial $M \in \mathbb{Q}[x]$ of* lowest degree *with $M(\alpha) = 0$, called the* minimal polynomial of α over $\mathbb{Q}$. *Furthermore, every polynomial in $\mathbb{Q}[x]$ vanishing at α is divisible by M.*

Definition 2.2. The *conjugates* of $\alpha \in \overline{\mathbb{Q}}$ over $\mathbb{Q}$ are the roots of M.

Question 2.3. Can you generalize these notions to base fields K other than $\mathbb{Q}$?

Proposition-Definition 2.4. *The minimal polynomial of $\alpha \in \overline{\mathbb{Q}}$ lies in $\mathbb{Z}[x]$ if and only if $P(\alpha) = 0$ for some* monic *polynomial $P \in \mathbb{Z}[x]$. In this case, α is called an* algebraic integer.

Definition 2.5. $\mathbb{Q}[\alpha, \beta, \dots]$ is the set of $\mathbb{Q}$-coefficient polynomial expressions in $\alpha, \beta, \dots$, while $\mathbb{Q}(\alpha, \beta, \dots)$ is the set of fractions of such expressions (with nonzero denominator).

Problem 2.6. Prove the fundamental theorem of symmetric sums.

Problem 2.7 (Resultant)**.** Find a polynomial R in the coefficients $a_1, b_1, \dots$ of $f = x^n + a_1x^{n-1} + \cdots \in \mathbb{C}[x]$ and $g = x^m + b_1x^{m-1} + \cdots \in \mathbb{C}[x]$ such that f, g share a common zero if and only if $R(a_1, b_1, \dots) = 0$.

Problem 2.8. If $\alpha \in \overline{\mathbb{Q}}$, and $\beta \in \mathbb{Q}[\alpha]$ is nonzero, then $\beta^{-1} \in \mathbb{Q}[\alpha]$. Consequently, $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, i.e. rational fractions in α can be written as polynomials in α.[1]

Problem 2.9 (Asked by Luke in "Manip" class)**.** If $\alpha \in \overline{\mathbb{Q}}$ has conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, show that $\prod_{2 \le j \le n} P(\alpha_j) \in \mathbb{Q}[\alpha_1]$ for any polynomial $P \in \mathbb{Q}[x]$.

Problem 2.10. The sum and product of two algebraic numbers is still algebraic. The reciprocal of any nonzero algebraic number is algebraic.

Problem 2.11. Prove the fundamental theorem of algebra algebraically.

Theorem 2.12 (Primitive element theorem)**.** *If $\alpha, \beta \in \overline{\mathbb{Q}}$, then there exists $\gamma \in \overline{\mathbb{Q}}$ such that $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$.*

Problem 2.13 (Nagell?)**.** If $f, g \in \mathbb{Q}[x]$ are *non-constant*, then there exist infinitely many primes p such that $v_p(f(m), g(n)) \ge 1$ for some pair of integers (m, n).

Problem 2.14 (Algebraic tower)**.** Show that all roots of a polynomial $f \in \overline{\mathbb{Q}}[x]$ lie in $\overline{\mathbb{Q}}$.

2.2. **Special number fields: radical and cyclotomic extensions.**

Problem 2.15 (2013-2013 Winter OMO, W.)**.** Find the remainder when $\prod_{i=0}^{100}(1 - i^2 + i^4)$ is divided by 101.

Problem 2.16 (W.)**.** Let $\omega = e^{2\pi i/5}$ and $p > 5$ be a prime. Show that $\frac{1+\omega^p}{(1+\omega)^p} + \frac{(1+\omega)^p}{1+\omega^p}$ is an integer congruent to $2 \pmod{p^2}$.

Problem 2.17 (Totally real subfield of cyclotomic number field)**.** Let $n \ge 3$. Compute the minimal polynomial and conjugates $\alpha_1, \alpha_2, \ldots$ of $\zeta_n + \zeta_n^{-1}$. Show that these conjugates generate $\mathbb{R} \cap \mathbb{Q}[\zeta_n]$ over $\mathbb{Q}$, meaning $\mathbb{R} \cap \mathbb{Q}[\zeta_n] = \mathbb{Q}[\alpha_1, \alpha_2, \ldots]$.

Problem 2.18 (Heard from Yang)**.** Find all integers $n \ge 2$ such that $2^{1/n}$ is a sum of roots of unity.

Problem 2.19. Find a constant $c > 0$ such that $\sqrt{2}$ is at least cq^{-2} away from any rational number of denominator at most q. Can you generalize this?

Problem 2.20. Let d be a non-square integer. Prove that *Pell's equation*, $x^2 - dy^2 = 1$, has a nontrivial integer solution $(x, y) \ne (\pm 1, 0)$.

Problem 2.21 (Carl Lian, HMIC 2015/5)**.** Let $\omega = e^{2\pi i/5}$. Prove that there do not exist $a, b, c, d, k \in \mathbb{Z}$ with $k > 1$ such that $(a + b\omega + c\omega^2 + d\omega^3)^k = 1 + \omega$.

Problem 2.22 (Lucas)**.** If $p \ge 3$ is prime, then $\Phi_p(x) = U_p(x)^2 - (-1)^{(p-1)/2} p x V_p(x)^2$ for some $U_p, V_p \in \mathbb{Z}[x]$ of degree $(p-1)/2$ and $(p-3)/2$, respectively.

Problem 2.23 (Kronecker)**.** If $f \in \mathbb{Z}[x]$ is monic with all roots in the unit disk, then the roots are all roots of unity.

Problem 2.24 (HMIC 2014/4)**.** Let ω be a root of unity and f be a polynomial with integer coefficients. Show that if $|f(\omega)| = 1$, then $f(\omega)$ is also a root of unity.

Problem 2.25. If $f \in \mathbb{Z}[x]$ is monic with all roots real in $[-2, 2]$, then all its roots are of the form $2\cos(2k\pi/n)$ for some integers $k \ge 0$ and $n \ge 1$.

Problem 2.26 (China?)**.** Find all *monic* polynomials $P \in \mathbb{Z}[x]$ with all roots *real*, in $(0, 3)$.

Problem 2.27. Motivate the solution of a cubic equation, using a roots of unity filter.

[1] In particular, $\mathbb{Q}[\alpha]$ is a *field*.

2.3. Ramification and extended valuations in cyclotomic extensions.

Problem 2.28. Let $\zeta = e^{2\pi i/p}$ for some prime p. From $(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}) = p$, what can you say about $\frac{(1-\zeta)^{p-1}}{p}$ as an algebraic number? (Something similar works for prime powers, but not for other numbers.)

Problem 2.29 (Ring of integers $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ in pth cyclotomic field)**.** Let p be a prime. If $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ is an algebraic integer, where $a_i \in \mathbb{Q}$, then $a_i \in \mathbb{Z}$ for all i.

Theorem 2.30 (Gauss)**.** *$\sum_{n=0}^{p-1} \zeta_p^{n^2}$ is $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $i\sqrt{p}$ if $p \equiv 3 \pmod 4$.*

Problem 2.31 (1996 ISL)**.** Let n be an even positive integer. In terms of n, determine the set of positive integers k such that $k = f(x)(x+1)^n + g(x)(x^n+1)$ for some $f, g \in \mathbb{Z}[x]$.

Problem 2.32 (W., adapted from Gabriel Dospinescu, PFTB, 2010 MR U160)**.** Let p be a prime and let n, s be positive integers. Prove that $v_p\left(\sum_{p \mid k, 0 \le k \le n} (-1)^k k^s \binom{n}{k}\right) \ge v_p(n!)$.

3. Galois theory

Problem 3.1. An extension $K = \mathbb{Q}(\alpha)$ is called *Galois* over $\mathbb{Q}$ if $\beta \in K$ for all conjugates β of α over $\mathbb{Q}$. Prove that $K/\mathbb{Q}$ is Galois if and only if it is the smallest field in which the minimal polynomial $M \in \mathbb{Q}[x]$ of α factors completely (i.e. K is the *splitting field* of M over $\mathbb{Q}$); if and only if there are exactly $\deg M$ field automorphisms of K fixing $\mathbb{Q}$.

Problem 3.2 (Vandermonde, Galois)**.** Let α be an algebraic number and let $\beta \in \mathbb{Q}[\alpha]$ be a $\mathbb{Q}$-coefficient polynomial expression $P(\alpha)$ in α that remains invariant when α is replaced with any conjugate of α. Prove that $\beta \in \mathbb{Q}$.

Problem 3.3. Solve a general cubic and quartic equation in radicals, using finite Fourier analysis on certain abelian group quotients of S_3 and S_4, respectively.

For the next problem, let $K/\mathbb{Q}$ be a number field with a $\mathbb{Q}$-*algebra automorphism*[2] $\sigma\colon K \to K$ that is *cyclic Galois* of order d, so that $\sigma^d = \mathrm{Id}$ and for any element $\alpha \in K$, the list $\alpha, \sigma\alpha, \ldots, \sigma^{d-1}\alpha$ contains all the roots of the minimal polynomial of α over $\mathbb{Q}$.

Problem 3.4 (Hilbert's theorem 90)**.** If $K/\mathbb{Q}$ is *cyclic* as specified above, prove that $\alpha \in K$ satisfies $\prod_{k=0}^{d-1} \sigma^k\alpha = 1$ if and only if there exists nonzero $z \in K$ such that $\alpha = z/\sigma z$.

[2]meaning a $\mathbb{Q}$-linear isomorphism preserving multiplication and the identity