S.T. Yau College Student Mathematics Contests 2019
Algebra and Number Theory Team

1. (a) Let p be a (positive) prime integer, and $P \in \mathbb{Q}[X]$ an irreducible polynomial of degree p having two complex conjugate roots and $(p-2)$ real roots. Let K the subfield of $\mathbb{C}$ generated by the roots of P. Prove that K is a Galois extension of $\mathbb{Q}$, whose Galois group is the symmetric group on p elements.

(b) What is the Galois group of the polynomial $P(X) = X^5 - 6X + 3$?

2. Let K be a **nonalgebraically** closed field. Let $f_1, f_2, \ldots, f_m \in K[x_1, \ldots, x_n]$ and let $S \subset K^n$ be the set of solutions of the system of equations $f_1 = \cdots = f_m = 0$. Show that there exists a polynomial P such that S is the set of solutions of the equation $P = 0$.

3. (a) Let K be a field and $K[X]$ the ring of polynomials with coefficients in K. Define $v_0 : K[X] - \{0\} \to \mathbb{N}$ by the rule

$$v_0\Big(\sum_{0 \le k \le d} a_k X^k \Big) \;=\; \min\{\, k |\ a_k \neq 0 \,\} \,.$$

Fix a real number $C > 1$ (the particular choice will not matter). For $p \in K[X]$, define $\|p\|_0 = c^{-v_0(p)}$ if $p \neq 0$, and $\|0\|_0 = 0$. Show that

$$d_0(p, q) \;=\; \|p - q\|_0$$

defines an ultrametric on $K[X]$. Recall the notion of an ultrametric: a metric $d(\ ,\ )$ such that $d(p, r) \le \max\big(d(p, q)\,,\, d(q, r) \big)$ for all $p,\ q,\ r\ \in\ K[X]$.

(b) A **formal power series** with coefficients in K is a formal sum

$$\sum_{k=0}^{\infty} a_k\, X^k \quad , \quad a_k \in K \ .$$

The set $K[[X]]$ of all formal power series is a commutative ring with 1 under formal addition and multiplication of series. Note that every polynomial can be regarded as a formal power series, with only finitely many non-zero coefficients; thus $K[X] \subset K[[X]]$.

Show that v_0, $\|\ \|_0$, and d_0 extend naturally from $K[X]$ to $K[[X]]$ and identify $K[[X]]$ with the completion of $K[X]$: a metric space containing $K[X]$ whose metric agreeds with d_0 on $K[X]$, such that $K[X]$ is dense in the completion.

(c) Prove that $K[[X]]$, equipped with the ultrametric $d_0(\ ,\ )$, is a compact metric space, provided the field K is finite.

4. A integer n is said to be a **Congruent Number** if it is the area of a right triangle with each of the three sides rational numbers. For example, 6 is a congruent number since it is the area of the right triangle of sides length $(3, 4, 5)$.

Prove the following:

(a) $n \in \mathbb{N}$ is a congruent number if and only if there exist $m, a, b \in \mathbb{N}$ such that

$$nm^2 = ab(a+b)(a-b)$$

(b) For each of $r \in \{1, 2, 3, 5, 6, 7\}$, there exists infinitely many square free congruent numbers $n \equiv r \pmod 8$.

5. Let R be a commutative ring, and suppose

$$0 \to K \longrightarrow P \xrightarrow{f} M \to 0 \qquad \text{and} \qquad 0 \longrightarrow K' \longrightarrow P' \xrightarrow{f'} M \to 0$$

are short exact sequences with P and P' projective. Prove that $K \oplus P'$ is isomorphic to $K' \oplus P$.

Hint. With the indicated f and f', consider $Z = \{(p, p') \in P \oplus P'; f(p) = f'(p')\}$ and the natural maps from Z to P and P'.)