Math 80220 Algebraic Number Theory
Problem Set 6

Andrei Jorza

due Wednesday, April 23

1. Let $f \in \mathbb{Z}[X]$ be a nonzero polynomial such that for all but finitely many primes p the polynomial $f \bmod p$ splits into linear factors in $\mathbb{F}_p[X]$.
   (a) If f is irreducible and K is the splitting field of f show that for all but finitely many primes p the element $\mathrm{Frob}_{\mathfrak{p}/p} = 1$ for $\mathfrak{p} \mid p$ prime ideal of K and conclude that $\deg f = 1$. [Hint: Chebotarev.]
   (b) Show that f splits into linear factors in $\mathbb{Z}[X]$.

2. (a) (Optional, but you'll need it for part 2b) Let G be a group acting faithfully (i.e., $G \to \mathrm{Aut}(X)$ is injective) and transitively (i.e., for any x, y there exists g such that $gx = y$) on a finite set X with more than one element.
      i. If every $g \in G$ has a fixed point, i.e., $x \in X$ such that $gx = x$, show that $G = \cup_{x \in X} \mathrm{Stab}_G(x) = \cup_{g \in G} g \,\mathrm{Stab}_G(x_0) g^{-1}$ for a fixed x_0.
      ii. If H is the maximal proper subgroup of G containing $\mathrm{Stab}_G(x_0)$ show that H is not normal.
      iii. Deduce that the normalizer $N_G(H) = H$ and thus that $\{gHg^{-1} | g \in G\} = \{gHg^{-1} | g \in G/H\}$.
      iv. Deduce that $\cup gHg^{-1}$ has at most $(|H| - 1)[G : H] + 1$ elements.
      v. Derive a contradiction and conclude that there exists $g \in G$ such that g has no fixed points.
   (b) Suppose $f \in \mathbb{Z}[X]$ is a monic irreducible polynomial such that $f \mod p$ has a root in $\mathbb{F}_p$ for all but finitely many primes p.
      i. Let $K/\mathbb{Q}$ be the splitting field of f, i.e., the extension of $\mathbb{Q}$ generated by the roots of f. If $\deg f > 1$ show that there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) \neq \alpha$ for every root α of f.
      ii. Show that there exist infinitely many primes p such that Frob_p is the conjugacy class of σ.
      iii. Show that for all but finitely many p, Frob_p has a fixed point and deduce that f is linear.

3. (a) Show that $f(X) = (X^2 - 2)(X^2 - 3)(X^2 - 6)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$. [Hint: $\mathbb{F}_p^\times$ is cyclic.]
   (b) Show that $f(X) = (X^3 - 2)(X^2 + X + 1)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$. [Hint: treat $p \equiv \pm 1 \pmod 3$ separately.]
   (c) Show that if $f(X)$ has a root in $\mathbb{F}_p$ for every prime p but no root in $\mathbb{Z}$ then $\deg f \geq 5$. [Hint: Use 2 to reduce to a product of two quadratics and recall that $X^2 - a$ has a root $\bmod p$ if and only if $\mathrm{Frob}_p = 1$ in $\mathbb{Q}(\sqrt{a})$.]

4. For an integer $n \geq 1$ let $\ell(n)$ be the length of the period of $1/n$ written in decimal notation. For example, $1/2 = 0.5$ so $\ell(2) = 0$, $1/12 = 0.08(3)$ so $\ell(12) = 1$ and $1/675 = 0.00(148)$ so $\ell(675) = 3$. The purpose of this problem is to show that $\ell(p)$ is an odd number for one third of the primes p.
   (a) Show that if $(n, 10) = 1$ then $\ell(n)$ is the order of 10 in $(\mathbb{Z}/n\mathbb{Z})^\times$.
   (b) Let $p \nmid 10$ and $k \geq 1$. Show that p splits completely in $\mathbb{Q}(\zeta_{2^k})$ but not in $\mathbb{Q}(\zeta_{2^{k+1}})$ if $p - 1 = 2^k m$ where m is odd.

(c) Let $n \geq 2, d \geq 1$ be integers and a be a square-free integer. Show that $K = \mathbb{Q}(\sqrt[n]{a}, \zeta_{nd})$ is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/nd\mathbb{Z})^\times \rtimes \mathbb{Z}/n\mathbb{Z}$.

(d) Suppose $p = 2^k m$ as above and assume that $X^{2^k} \equiv 10 \pmod{p}$ has a solution in $\mathbb{F}_p$. Show that p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$. [Hint: What is the minimal polynomial of $\sqrt[2^k]{10}$ over $\mathbb{Q}(\zeta_{2^k})$?]

(e) Reciprocally, if $p \nmid 10$ and $k \geq 1$ show that p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ implies that 2^k is the largest power of 2 in $p-1$ and $X^{2^k} \equiv 10 \pmod{p}$ has a solution in $\mathbb{F}_p$. [Hint: You may use the fact that if p splits completely in K and L then it does so in the composite KL.]

(f) Deduce that $\ell(p)$ is odd if and only if p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ for some $k \geq 1$.

(g) Show that $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})/\mathbb{Q}$ is Galois of order 2^{2k-1} and $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})/\mathbb{Q}$ is Galois of order 2^{2k}.

(h) Show that the density of primes p such that $\ell(p)$ is an odd number is $1/3$. [Hint: Recall that splitting completely means trivial Frobenius.]

For more about this problem see Odoni, "A Conjecture of Krishnamurty on decimal periods and some allied problems". You are more than welcome to try to decipher that paper to figure out a solution for this problem (which is a very special case of that paper).

5. Let K be a number field and $f \in \mathcal{O}_K[X]$ be an irreducible monic polynomial with roots $\alpha_1, \ldots, \alpha_n$. Let $L = K(\alpha_1, \ldots, \alpha_n)$ be its splitting field. Recall that the Galois group $G = \mathrm{Gal}(L/K)$ permutes the roots α_i and this gives an injection $G \hookrightarrow S_n$.

(a) Let $\mathfrak{p}$ be a prime ideal such that $f \mod \mathfrak{p} \in k_\mathfrak{p}[X]$ is separable, i.e., has distinct roots (this happens for all but finitely many $\mathfrak{p}$, the ones not dividing the discriminant of f). Let $\mathfrak{q} \mid \mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$. Show that the decomposition group $D_{\mathfrak{q}/\mathfrak{p}}$ as a subgroup of the permutation group of the roots $\alpha_1, \ldots, \alpha_n$ of f is isomorphic to $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$ as a subgroup of the permutation group of the roots $\alpha_1 \mod p, \ldots, \alpha_n \mod p$ of $f \mod p$.

(b) For $\mathfrak{p}$ as above show the cycle structure of an element of the conjugacy class $\mathrm{Frob}_\mathfrak{p}$ as a permutation of the roots of n (cycle structure here means the multiset of lengths of the cycles) is given by the degrees of the irreducible factors of $f \mod \mathfrak{p} \in k_\mathfrak{p}[X]$. [Hint: Frobenius generates the Galois groups of finite fields.]

(c) (Do one of 5c, 5d, 5e) Consider the polynomial $f(X) = X^5 - X + 1$.

i. Show that f is irreducible over $\mathbb{Q}$. [Hint: Show that it is irreducible over $\mathbb{F}_5$.]

ii. Show that the splitting field of f has Galois group S_5 over $\mathbb{Q}$. [Hint: S_5 is generated by a 5-cycle and a transposition.]

iii. For each partition $5 = \sum i_k$ let $n_{i_1,\ldots,i_k}$ be the number of permutations with cycle structure $(i_1, \ldots, i_k)$. For example $n_{1,1,1,1,1} = 1$ and $n_{2,1,1,1} = \binom{5}{2} = 10$. Also let $\mathcal{P}_{i_1,\ldots,i_k}$ be the set of primes p such that $f \mod p = f_{i_1} \cdots f_{i_k}$ in $\mathbb{F}_p[X]$ where f_{i_j} is irreducible of degree i_j. Show that

$$\delta(\mathcal{P}_{i_1,\ldots,i_k}) = \frac{n_{i_1,\ldots,i_k}}{120}$$

iv. In particular, show that for one sixth of primes p, $f \mod p$ factors as a quadratic times a cubic and for one fifth of primes p, f is irreducible in $\mathbb{F}_p[X]$.

(d) (Do one of 5c, 5d, 5e) Let $N > 1$ be an integer and $\Phi_N(X)$ be the N-th cyclotomic polynomial, i.e., the minimal polynomial of ζ_N.

i. If $p \nmid N$ is a prime show that $\Phi_N(X) \mod p$ factors as a product of irreducible polynomials of the same degree $d \mid \varphi(N)$.

ii. Let n_d be the number of $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ of order d. Show that the density of primes p such that $\Phi_N \mod p$ factors as a product of polynomials of degree $d \mid \varphi(N)$ equals $\dfrac{n_d}{D(\varphi(N))}$ where $D(n)$ is the number of divisors of n.

iii. Write $N = 2^k p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorization of N. If $4 \nmid N$ suppose that $r \geq 2$ and if $4 \mid N$ suppose that $r \geq 1$. Show that the set of primes p which are inert in $\mathbb{Q}(\zeta_N)$ has density 0. [Hint: What is $(\mathbb{Z}/N\mathbb{Z})^\times$ as a product of cyclic groups?]

(e) (Do one of 5c, 5d, 5e) Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial of degree n with Galois group S_n. Suppose

$$n = \underbrace{n_1 + \cdots + n_1}_{m_1} + \cdots + \underbrace{n_k + \cdots n_k}_{m_k}$$

where $n_1 > \cdots > n_k \geq 1$. Show that the density of primes such that $f \mod p = \prod f_i$ with $(\deg f_i) = (n_1, \ldots, n_1, \ldots, n_k, \ldots, n_k)$ (up to permutation) is

$$\frac{1}{\prod n_i^{m_i} \prod m_i!}$$