Problems in algebraic number theory

Daniel Miller

May 2, 2017

1 Class field theory

Problem 1 (Ravi)**.** *What is the smallest n such that the degree n unramified extension of $\mathbb{Q}_p$ has an abelian totally ramified extension of degree q, where p and q are distinct primes?*

I claim that the degree n unramified extension of $\mathbb{Q}_p$ has an abelian totally ramified extension of degree q if and only if $p^n = 1$ in $\mathbb{F}_q$.

Proof. Let k_n be the degree n unramified extension of $\mathbb{Q}_p$. Recall [3, V.1.4] that local class field theory yields an order-reversing bijection between abelian extensions of k_n of degree q and open subgroups of $k_n^\times$ of finite q. By [3, II.5.7], one sees that

$$k_n^\times \simeq \mathbb{Z} \times \mathbb{Z}/(p^n - 1) \times \mathbb{Z}_p^n$$

We are interested in open $U \subset k_n^\times$ of index q, i.e. continuous surjections $k_n^\times \twoheadrightarrow \mathbb{Z}/q$. If we have such an open subgroup, clearly one has $\mathbb{Z}_p^n \subset U$. By [3, V.1.7], if L/k_n is the extension induced by U, one has L/k ramified if and only if $\mathbb{Z}/(p^n - 1) \times \mathbb{Z}_p^n \not\subset U$. In particular, $\mathbb{Z}/(p^n - 1) \to \mathbb{Z}/q$ must be nonzero. This can occur if and only if $q \mid p^n - 1$, i.e. p has order n in $\mathbb{F}_q^\times$. □

Problem 2 (Ravi)**.** *How many C_{13} extensions are there of $\mathbb{Q}(i)$ ramified only at (primes above) 13? What about $C_{13} \times C_{13}$ extensions?*

Problem 3 (Ravi)**.** *Can a C_2 extension of $\mathbb{Q}$ ramified at only one prime have even class number?*

2 General nonsense

Problem 4 (Myself)**.** *Let A be a noetherian domain such that $\mathfrak{ab} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b})$ for all ideals $\mathfrak{a}, \mathfrak{b} \subset A$. Does it follow that A is dedekind?*

The answer is yes, and in some generality. I claim that if A is a domain for which $\mathfrak{ab} = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b})$ for all ideals $\mathfrak{a}, \mathfrak{b}$, then A is a prüfer ring.

Proof. (**NOTE:** This proof is essentially taken from an answer on math.stackexchange, which should be referenced.)

Recall (cf. [1, VII §2 ex.12]) that a domain A is a *prüfer ring* if for all prime ideals $\mathfrak{p} \subset A$, $A_\mathfrak{p}$ is a valuation ring. It is known that A is prüfer if and only if each finitely generated ideal is invertible. Note that principal ideals are trivially invertible. So, it suffices to prove that if $\mathfrak{a}, \mathfrak{b}$ are invertible and $\mathfrak{ab} = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})$, then $\mathfrak{a} + \mathfrak{b}$ is invertible. But one has

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b})\mathfrak{a}^{-1}\mathfrak{b}^{-1} = \mathfrak{ab}\mathfrak{a}^{-1}\mathfrak{b}^{-1} = 1$$

so $\mathfrak{a} + \mathfrak{b}$ is invertible. If $\mathfrak{a} \subset A$ is an arbitrary finitely generated ideal, just do induction on the number of generators of $\mathfrak{a}$ to obtain the result. □

Problem 5 (Myself)**.** *Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial that has a root in $\mathbb{Q}_p$ for all $p \leqslant \infty$. Does it follow that f has a root in $\mathbb{Q}$?*

The answer is yes, and in some generality. Let $K = \mathbb{Q}(x)$, where x is some root of f. If K is unramified at p, then f has a root modulo p if and only if there is a prime $\mathfrak{p} \mid p$ in K with $f_{\mathfrak{p}/p} = 1$. We will prove that the set of such p has (Dirichlet) density < 1.

Proof. First, we recall the definition of density for sets of primes. Let k be a number field and S a set of primes in k. The (Dirichlet) *density* of S is the limit

$$d(S) = \lim_{s \to 0^+} \frac{\sum_{\mathfrak{p} \in S} N(p)^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}}.$$

Now K/k be an arbitrary extension of number fields, and L/k the Galois closure of K. Let $P(K/k)$ be the set of primes $\mathfrak{p}$ of k for which there is $\mathfrak{q} \mid \mathfrak{p}$ with $f_{\mathfrak{q}/\mathfrak{p}} = 1$. I claim that $P(K/k)$ has density at most $1 - \frac{1}{n}$, where $n = [L : k]$.

For $\sigma \in G = \mathrm{Gal}(L/k)$, let $P_{L/k}(\sigma)$ be the set of primes $\mathfrak{p}$ in k with some $\mathfrak{q} \mid \mathfrak{p}$ with $\sigma = \left(\frac{L/k}{\mathfrak{q}}\right)$. Lemma 13.5 of [3] implies

$$dP(K/k) = \sum_{[\sigma] \cap H \neq \varnothing} dP_{L/k}(\sigma)$$

where $H = \mathrm{Gal}(L/K)$ and $[\sigma]$ is the conjugacy class of σ in G. The Čebotarev density theorem [3, VII.13.4] says that $dP_{L/k}(\sigma) = \#[\sigma]/n$. As a result, we have

$$dP(K/k) = \frac{1}{n} \sum_{[\sigma] \cap H \neq \varnothing} \#[\sigma] \leqslant \frac{1}{n} \left| \bigcup_{g \in G} gHg^{-1} \right| \leqslant \frac{1}{n}(\#G - 1)$$

the last inequality coming from the elementary fact that a finite group is not the union of conjugates of any proper subgroup. □

Problem 6 (Myself)**.** *Let A be an abelian variety over an algebraically closed field k. Is there an upper / lower bound on the genus of curves that can embed into A?*

The answer is about as good as can be hoped for. If $C \subset A$ is a curve, then the genus g of C can be bounded as: $d_{\min} \leqslant g \leqslant d$, where $d_{\min}$ is the smallest dimension of a nonzero sub-abelian variety of A, and $d = \dim A$.

Proof. We only need a couple facts about abelian varieties and jacobians. The first is Poincare's reducibility theorem [2, 19.1]. If $B \subset A$ are abelian varieties, then there is an abelian variety $B' \subset A$ such that $B \times B' \to A$ is an isogeny (so in particular $A = B + B'$ and $B \cap B'$ is finite). Recall that if C is a curve, the jacobian J of C is an abelian variety of dimension $g = g(C)$, which comes with a canonical embedding $C \hookrightarrow J$, such that any map $C \to A$ to an abelian variety that sends 0 to 0 factors uniquely through J. (Here, $0 \in C$ is the element that maps to $0 \in J$.)

Suppose $C \hookrightarrow A$. We get a map $J \to A$, the kernel of which is abelian subvariety of J, hence it has a complement K'. Consider the composite

$$C \hookrightarrow J \twoheadrightarrow K' \hookrightarrow J \to A$$

□

Problem 7 (Myself)**.** *Let S be a connected variety over an algebraically closed field k. If $X \to S$ is a one-to-one etale cover, is X an isomorphism?*

The answer is yes, and in greater generality.

Proof. Let S be a scheme for which Grothendieck's galois theory works. Let $s \to S$ be a geometric point. If $f : X \to S$ is an etale cover, then we get an action of $\pi_1(S, s)$ on the fiber $F_s(X) = |X \times_S s|$. Under our hypotheses, this is a single point, so the action of $\pi_1(S)$ is trivial. But $X \to S$ is determined by $F_s(X)$, so $X \simeq S$. □

3 Elementary number theory

Problem 8 (Myself)**.** *Show that for all primes p and integers n, $v_p(n!) \leqslant n$.*

Proof. A simple computation suffices:

$$v_p(n!) = \sum_{r \geqslant 1} \left\lfloor \frac{n}{p^r} \right\rfloor \leqslant \sum_{r \geqslant 1} \frac{n}{p^r} = \frac{n}{p-1} \leqslant n.$$

□

References

[1] Bourbaki, N. *Commutative Algebra: Chapters 1-7*, Springer, 1989.

[2] Mumford, D. *Abelian Varieties*, Tata Inst. Fund. Research, 1974.

[3] Neukirch, J. *Algebraic Number Theory*, Springer, 1999.