The Chebotarev Density Theorem

Hendrik Lenstra

1. Introduction

Consider the polynomial $f(X) = X^4 - X^2 - 1 \in \mathbb{Z}[X]$. Suppose that we want to show that this polynomial is irreducible. We reduce f modulo a prime p and hope to show that it is irreducible as an element of $\mathbb{Z}/p\mathbb{Z}[X]$, so then f is irreducible in $\mathbb{Z}[X]$. We see that $f \equiv (X^2 + X + 1)^2 \pmod 2$—let us disregard the exceptional cases where a multiple root occurs, those primes dividing the discriminant $\Delta(f)$. Modulo 3, however, we see that f is irreducible because it has no root in $\mathbb{F}_9$. Sometimes for a polynomial one can combine information gleaned from several primes: it would suffice, for example, to show that our polynomial f is the product of a linear and cubic factor modulo one prime and the product of 2 quadratic factors modulo another.

We are then posed with the question: given a polynomial f, among the factorization patterns of f modulo many primes (throwing out the cases when a double factor occurs), how often does each occur? We will be able to obtain an answer to this question as an application of the Chebatorev density theorem.

As an illustration, we gather a bit of data. Along with the polynomial $X^4 - X^2 - 1$, let us also consider $X^4 - X - 1$. Consider the following:

f	p_0	$\Delta(f)$	$\#\{p \le p_0 : p \nmid \Delta(f),\ p \text{ prime}\}$
$X^4 - X^2 - 1$	7933	$-2^4 \cdot 5^2$	1000
$X^4 - X - 1$	7927	-283	1000

We then tabulate how often each factorization pattern occurs among all primes up to p_0:

f	4	1, 3	2, 2	1, 1, 2	1, 1, 1, 1
$X^4 - X^2 - 1$	254	0	379	251	116
$X^4 - X - 1$	258	337	117	253	35

For example, there are 254 primes p up to 7933 such that $f = X^4 - X^2 - 1$ remains irreducible modulo p, and 251 primes such that f splits into two linear factors and one quadratic factor. Note that the pattern $1, 3$ does not occur for the first polynomial because if x is a root, then so is $-x$.

Notice that the fractions that occur are very close to much simpler ones. We might guess that the fraction of each factorization pattern is in fact asymptotically given by:

f	4	1, 3	2, 2	1, 1, 2	1, 1, 1, 1
$X^4 - X^2 - 1$	1/4	0	3/8	1/4	1/8
$X^4 - X - 1$	1/4	1/3	1/8	1/4	1/24

The Chebotarev density theorem will allow us to explain this striking phenomenon?

2. Frobenius

We begin by looking at the Frobenius element. In the case of an abelian extension $K \subset L$, we have an Artin symbol $A(\mathfrak{p}) \in \mathrm{Gal}(L/K)$ for primes $\mathfrak{p} \nmid \Delta_{L/K}$, with the unique property that for all $\alpha \in \mathcal{O}_L$,

$$A(\mathfrak{p})(\alpha) \equiv \alpha^{\#\mathcal{O}_K/\mathfrak{p}} \pmod{\mathfrak{p}\mathcal{O}_L}.$$

This element $A(\mathfrak{p})$ is often called the Frobenius at $\mathfrak{p}$.

If you drop the condition that L/K is abelian and insist only that it be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, then the definition of the Artin map depends on a choice of prime $\mathfrak{q}$ lying over the prime $\mathfrak{p}$. Upon this choice, when $\mathfrak{p} \nmid \Delta_{L/K}$, there is a unique $\mathrm{Frob}_\mathfrak{q} \in G$ such that for all $\alpha \in \mathcal{O}_L$,

$$\mathrm{Frob}_\mathfrak{q}(\alpha) \equiv \alpha^{\#\mathcal{O}_K/\mathfrak{p}} \pmod{\mathfrak{q}}.$$

This really does depend on the choice of $\mathfrak{q}$: given another choice $\mathfrak{q}' \mid \mathfrak{p}$, there is an element $\sigma \in \mathrm{Gal}(L/K)$ such that $\mathfrak{q}' = \sigma(\mathfrak{q})$, and we then see that $\mathrm{Frob}_{\mathfrak{q}'} = \sigma \,\mathrm{Frob}_\mathfrak{q}\, \sigma^{-1}$. In this case, we must treat not just the elements themselves but the entire conjugacy class.

We define the *Frobenius symbol of* $\mathfrak{p}$ *in* L/K to be the conjugacy class $\{\mathrm{Frob}_\mathfrak{q} : \mathfrak{q} \mid \mathfrak{p}\}$. Note that in the case of an abelian group, this set contains only a single element—though formally the element and the set containing this element are two different objects, we may identify the two. We will often abuse notation and denote by $\mathrm{Frob}_\mathfrak{p}$ any element of the conjugacy class and then treat it as something well-defined only up to conjugacy. We also denote $\mathrm{Frob}_\mathfrak{p}$ by $\sigma_\mathfrak{p}$.

The Frobenius element has several good properties. It restricts well to subfields: if $K \subset L$ and $L \subset M$ are Galois extension of fields, then $\sigma_\mathfrak{p} \in \mathrm{Gal}(M/K)$ maps by restriction to $\sigma_\mathfrak{p} \in \mathrm{Gal}(L/K)$.

Knowledge of $\sigma_\mathfrak{p}$ also allows us to control the decomposition of $\mathfrak{p}$ in every subfield. Given a subextension $K \subset E \subset L$, not necessarily Galois, write $\mathfrak{p}\mathcal{O}_E = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}$. Since $\mathfrak{p}$ is unramified, the decomposition of $\mathfrak{p}$ is given by the sequence of residue class degrees $f(\mathfrak{q}/\mathfrak{p})$. The Frobenius symbol tells you what they are: let $E = L^H$, fixed under the subgroup $H \subset G$. Then:

Fact 2.1. *The decomposition type of* $\mathfrak{p}$ *in* $\mathcal{O}_E$ *(i.e. the 'factorization pattern', which is a partition of the degree* $[E:K]$*) is equal to the cycle structure of* $\sigma_\mathfrak{p}$ *acting on* G/H*, where* $E = L^H$*.*

Note that G/H is a set of $[E:K]$ cosets. It comes with an action of G, hence a cycle structure of $\sigma_\mathfrak{p}$ on this set. Note that this cycle structure only depends on the conjugacy class of $\sigma_\mathfrak{p}$, which is an elementary fact from permutation theory.

Let $E = K(\alpha)$, $f \in \mathcal{O}_K[X]$ its minimal polynomial, and assume that $\mathfrak{p} \nmid \Delta(f)$. Then we have a very explicit description of the fact. On the one hand, the factorization pattern above is nothing other than the factorization pattern of $f \bmod \mathfrak{p}$ in $(\mathcal{O}_K/\mathfrak{p})[X]$. On the other hand, since α generates L over K, we see that for any τ, $\tau\alpha = \alpha$ if and only if $\tau \in H$, and $\tau_1\alpha = \tau_2\alpha$ if and only if $\tau_1 H = \tau_2 H$; so instead of the cycle structure on G/H, we may instead consider the cycle structure on the K-conjugates of α in L (namely, the zeros of f in L).

By concatenating, we can take the product of any distinct irreducible polynomials: we still have the fact that the factorization pattern of f modulo $\mathfrak{p}$ is the same as the cycle structure of $\sigma_\mathfrak{p}$ acting on the set of roots of f.

3. The Chebotarev Density Theorem

We now ask: given an element of the Galois group, can it be represented as a Frobenius of a prime? This is the question which is answered by the following theorem.

Theorem 3.1 (Chebotarev Density Theorem)**.** *Let* $K \subset L$ *be Galois, and let* $C \subset G = \mathrm{Gal}(L/K)$ *be a conjugacy class. Then*

$$\{\mathfrak{p} : \mathfrak{p} \text{ a prime of } K, \mathfrak{p} \nmid \Delta_{L/K}, \sigma_\mathfrak{p} \in C\}$$

has density $\#C/\#G$*.*

(In particular, this ratio is always > 0, so there always exist such primes.)

If S is a set of primes of K, then we define the *(natural) density* of S to be

$$d(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} : (\#\mathcal{O}_K/\mathfrak{p}) \le x, \mathfrak{p} \in S\}}{\#\{\mathfrak{p} : (\#\mathcal{O}_K/\mathfrak{p}) \le x, \mathfrak{p} \text{ prime}\}}$$

if this limit exists. If the natural density exists, then it is actually equal to the *(analytic) density*

$$d_{\mathrm{an}}(S) = \lim_{s\to 1^+} \frac{\displaystyle\sum_{\mathfrak{p}\in S} \frac{1}{\#(\mathcal{O}_K/\mathfrak{p})^s}}{\displaystyle\sum_{\mathfrak{p} \text{ prime}} \frac{1}{\#(\mathcal{O}_K/\mathfrak{p})^s}}.$$

The converse is not true, however, there are cases where the analytic density exists but the natural density does not. However, the Chebotarev Density Theorem is valid with either notion of density.

Therefore to explain the factorization data we found above, we must understand the conjugacy classes of G. For example, the factorization pattern $1,1,1,1$ occurs when $\sigma_{\mathfrak{p}}$ is the identity, which by the theorem occurs with frequency $1/\#G$. Therefore we guess that in the first case $\#G = 8$ and in the second $\#G = 24 = 4!$. We see then that the Galois group of $X^4 - X - 1$ must be S_4, and for this group there are six 4-cycles, occurring with frequency $6/24 = 1/4$, eight 3-cycles, with frequency $8/24 = 1/3$, and so on. For $X^4 - X^2 - 1$, we have the Sylow 2-subgroup of S_4, namely, D_8.

Indeed, this theorem goes both ways: if you know the densities, you can get information about the Galois group, and if you know the group, you can predict the densities that occur by computing the set of conjugacy classes of the group.

If you apply this theorem in the abelian case, and combine the Chebotarev density theorem with the classification of abelian extensions that comes from Galois theory, then you get statements that are quite independent of the extension L. For example, consider the extension $\mathbb{Q}(\zeta_m) \supset \mathbb{Q}$. We have the Galois group $G \cong (\mathbb{Z}/m\mathbb{Z})^*$, by the isomorphism $\sigma_p \leftrightarrow (p \bmod m)$. For any $a \bmod m \in (\mathbb{Z}/m\mathbb{Z})^*$, we see from the Chebotarev density theorem that $\{p : p \equiv a \bmod m\}$ has density $1/\phi(m)$, a statement which is a bit stronger than Dirichlet's theorem on primes in arithmetic progression.

We would like to generalize this to the setting of ray classes for a general algebraic number field, which leads to the description of cycles and the so-called Existence theorem, as discussed elsewhere.

Sometimes the Chebotarev density theorem applies to certain sets of primes, and sometimes not. Consider the set of odd primes p such that $2^{p-1} \equiv 1 \pmod{p^2}$; we do not know if it is finite or even cofinite, and is unlikely that one can apply the Chebotarev density theorem. Instead, we might consider for any quadratic form $aX^2 + bXY + cY^2 = f \in \mathbb{Z}[X,Y]$ the set $\{p : \exists\, x, y \in \mathbb{Z}, p = f(x,y)\}$. We look at the number field $E = \mathbb{Q}(\sqrt{D})$, where $D = b^2 - 4ac$. Assume D is a fundamental discriminant: then we consider E in its Hilbert class field $H(E)$. The structure of the group $G = \mathrm{Gal}(H(E)/\mathbb{Q})$ is under control, as we know $\mathrm{Cl}_E = \mathrm{Gal}(H(E)/E)$, and of course $\mathrm{Gal}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Therefore the primes occur with either frequency $1/(2h)$ or $1/h$, where $h = [H(E) : E] = \#\,\mathrm{Cl}_E$.

Exercises

Exercise 7.1. Let $f \in \mathbb{Z}[X]$ be a non-zero polynomial with the property that the polynomial $(f \bmod p) \in \mathbb{F}_p[X]$ splits completely into linear factors in $\mathbb{F}_p[X]$, for all but finitely many prime numbers p. Prove that f splits completely into linear factors in $\mathbb{Q}[X]$.

Exercise 7.2.

(a) Let G be a group acting transitively on a finite set Ω with $\#\Omega > 1$. Prove that there exists $\sigma \in G$ such that for all $\omega \in \Omega$ one has $\sigma\omega \neq \omega$.

(b) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial with the property that (f mod p) has a zero in $\mathbb{F}_p$, for all but finitely many primes p. Prove that f has degree 1.

Exercise 7.3. Find a monic polynomial $f \in \mathbb{Z}[X]$ of lowest possible degree such that (f mod p) has a zero in $\mathbb{F}_p$ for all prime numbers p but f has no zero in $\mathbb{Z}$.

Exercise 7.4. Let $f \in \mathbb{Z}[X]$, $f \notin \mathbb{Z}$. For a prime number p, let $n(p)$ be the number of distinct zeros of (f mod p) in $\mathbb{F}_p$. Prove that the average of $n(p)$, taken over all prime numbers p, is equal to the number of distinct monic irreducible factors of f in $\mathbb{Q}[X]$. (Your solution should include a rigorous definition of that 'average'.)

Exercise 7.5. Let K be an algebraic number field, with ring of integers A. Prove that the number of roots of unity in K is equal to the gcd of all numbers $\#(A/\mathfrak{p})-1$, where $\mathfrak{p}$ ranges over all prime ideals of A for which $A/\mathfrak{p}$ has characteristic greater than $1 + [K : \mathbb{Q}]$.

Exercise 7.6. Let R be the ring $\prod_p \mathbb{F}_p$, with p ranging over the set of all prime numbers. Prove that R has a maximal ideal $\mathfrak{m}$ for which the field $R/\mathfrak{m}$ has characteristic zero and contains an algebraic closure of $\mathbb{Q}$.

Exercise 7.7. Suppose $(S_n)_{n=1}^{\infty}$ is a sequence of sets of prime numbers with the property that $S_n \subset S_{n+1}$ for each n. Suppose also that each set S_n has a density $d(S_n)$. Does it follow that $S = \bigcup_n S_n$ has a density equal to $\sup_n d(S_n)$? Give a proof or a counterexample.

Exercise 7.8. Let S be the set of prime numbers for which $1/p$, when developed as a decimal fraction, has an odd period length. For example, one has $37 \in S$ because $1/37 = 0.027027027\ldots$, and $7 \notin S$ because $1/7 = 0.142857142857\ldots$. Prove that S has a density, and compute it.

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: hwl@math.leidenuniv.nl