Algebraic Number Theory

Madhav Nori, Summer 2007

Goal: Class Field Theory

What type of questions does one want to answer?

Consider a polynomial $f(x) \in \mathbb{Z}[x]$ of degree d,

$$f(x) = a x^d + b x^{d-1} + \cdots$$

Def: A prime number p is split for $f(x)$ if $p \nmid a$ and $\overline{f}(x) = \overline{a} \cdot \prod_{i=1}^{d} (x - \alpha_i)$ in $\mathbb{F}_p[x]$,

where $\overline{a}$ is the residue class of a mod p, and the α_i's are pairwise distinct elements of $\mathbb{F}_p$.

Define S_f to be the collection of all the split primes for f.

Question: What is S_f?

Variations. Replace $\mathbb{Z}$ by a commutative ring R and primes in $\mathbb{Z}$ by prime ideals in R. Then we can ask the same question.

The answer is known for some polynomials $f(x) \in \mathbb{Z}[x]$, and is called the Artin reciprocity law. We will state this result explicitly at some point.

Example 1. $f(x) = x^2 - 13$

It is clear that 2 is not split.

Hence a prime p is split for f if and only if p is odd and $\exists\, \alpha \in \mathbb{Z}$ s.t. $\alpha^2 \equiv 13 \pmod p$.

This is detected by the Legendre symbol:

p is split for $f \iff \left(\frac{13}{p}\right) = 1$.

By the Gauss reciprocity law,

$$\left(\frac{13}{p}\right) = 1 \iff \left(\frac{p}{13}\right) = 1 \iff p \text{ is a square modulo } 13$$

$$\iff$$ [illegible]

$$p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$$

Example 2. Let $n \in \mathbb{N}$ and consider $f(x) = x^n - 1$.

Then p is split for $f(x) \iff$

$$x^n - 1 = \prod_{i=1}^{n} (x - \alpha_i) \quad \text{in } \mathbb{F}_p[x]$$

where the α_i are pairwise distinct elements of $\mathbb{F}_p$ $\iff$ there are n distinct n-th roots of 1 in $\mathbb{F}_p$ $\iff n \mid (p-1)$

$$\iff p \equiv 1 \pmod n$$

Observe that in each of the two examples above, the split primes for f are precisely the primes in a union of finitely many arithmetic progressions of integers.

For more general rings we will need a suitable analogue of the notion of an arithmetic progression.

Background

- Basic properties of integral extensions
- $\mathbb{Z}_p$, $\mathbb{Q}_p$, and so on

We will prove the two fundamental finiteness theorems in the subject (the finiteness of the class number and the unit theorem, for number fields).

Some references

1) Borevich and Shafarevich
2) Lang's "Algebraic Number Theory"
3) Weil's "Basic Number Theory"
4) Cassels and Frölich, especially the chapters by Serre and Tate on local & global CFT.

Setup

R = principal ideal domain (usually $\mathbb{Z}$)

K = the fraction field of R

D = finite dimensional division algebra/K

Def: An R-order in D is a subring $A \subset R$ such that

(i) $R \subset A$

(ii) A is finitely generated as an R-module
($\Rightarrow A$ is free as an R-module)

(iii) $\forall d \in D$, $\exists\ 0 \neq c \in R$ s.t. $c \cdot d \in A$

$\Updownarrow$

(iii′) $K \otimes_R A \twoheadrightarrow D$ $\Longleftrightarrow$ (iii″) $K \otimes_R A \xrightarrow{\simeq} D$.

Example: $K = \mathbb{Q}$, $D = \mathbb{Q}(\sqrt{-1})$

$R = \mathbb{Z}$, $A = \mathbb{Z}[\sqrt{-1}]$

More generally: $d \in \mathbb{Z} \setminus \{0\}$, $D = \mathbb{Q}(\sqrt{d})$

$\Rightarrow$ we can take $A = \mathbb{Z} + \mathbb{Z} n\sqrt{d}$ $\forall n \in \mathbb{N}$.

Proposition. In the setup above, D always has an R-order.

(In fact, as we will see, it is not even necessary to assume that D is a division ring.)

Proof: Write $D = K\omega_1 \oplus \dots \oplus K\omega_n$ as a K-vector space. Write

$$\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\omega_k \qquad a_{ijk} \in K$$

Let $c \in R \setminus \{0\}$ be such that $ca_{ijk} \in R$ for all (i,j,k). Then

$$(c\omega_i)\cdot(c\omega_j) = \sum_{k=1}^{n} (ca_{ijk})(c\omega_k)$$

Therefore $A' := Rc\omega_1 + \dots + Rc\omega_n$ is a finitely generated R-submodule of D which is closed under multiplication. Now it is easy to check that $A := R + A'$ is an R-order for D. //

Remark: In general, orders in D need not be principal ideal domains. However, they are very close to being PIDs.

Theorem (Dirichlet): Let $R = \mathbb{Z}$, $K = \mathbb{Q}$, and let D be a finite dimensional division algebra over $\mathbb{Q}$, and A an order in D. (Hereafter, order $= \mathbb{Z}$-order.) Then the class set of A (defined below) is finite.

Def: Two left ideals $I_1, I_2 \subset A$ are said to be right principal equivalent if $\exists\, \alpha \in D$ with $I_1 \alpha = I_2$. The set of such equivalence classes (of nonzero left ideals) is called the class set of A.

Remark: We will see that if D is a number field and A is a maximal order in D, then the class set of A has a natural group structure (induced by multiplication of ideals).

Remark: If $I_1, I_2 \subset A$ are left ideals, then every A-module homomorphism $I_1 \longrightarrow I_2$ is given by $x \longmapsto x\alpha$ for some $\alpha \in D$. Thus Dirichlet's finiteness theorem can be restated as: the set of A-module isomorphism classes among the left ideals of A is finite.

Exercise (generalization of Dirichlet's theorem).

Let D be a finite dimensional semisimple algebra over $\mathbb{Q}$. Let V be a finitely generated left D-module. Let A be an order in D. Consider $X = \{ M \subset V \mid M \text{ is a finitely generated } A\text{-submodule} \}$

Then the set of isomorphism classes of A-modules appearing in X is finite.
(Use Wedderburn + Morita + Dirichlet.)

Proof of Dirichlet's theorem.

Idea: Consider a nonzero left ideal $I \subset A$. It is easy to see that A/I is finite.

Step 1. Find $0 \neq v \in I$ so that I/Av is "as small as possible".

We want to find $h \in \mathbb{N}$ so that $|I/Av| \leq h$.

We have $Iv^{-1} \supset AvV^{-1} = A$, and right multiplication by v^{-1} induces an isomorphism $I/Av \xrightarrow{\simeq} Iv^{-1}/A$ of left A-modules

What are the properties of Iv^{-1}?

(1) Iv^{-1} is a left A-module

(2) Iv^{-1} contains A

(3) $|Iv^{-1}/A| \leq h$.

We will check that there are only finitely many additive subgroups $J \subset D$ such that $A \subset J$ and $|J/A| \leq h$.

In fact, this is obvious, because any such J must be contained in $\frac{1}{h!}A \subset D$, and $(\frac{1}{h!}A)/A$ is finite $\therefore$ has only finitely many subgroups.

Upshot: We are reduced to the following

Proposition. There exists $h \in \mathbb{N}$ (depending only on D and A) such that for every left ideal $I \subset A$, there exists $v \in I$, $v \neq 0$ with $|I/Av| \leq h$.

We begin the proof of this proposition.

Claim 1. Let $T \in \mathrm{Mat}_n(\mathbb{Z})$, $\det(T) \neq 0$. Then $\mathbb{Z}^n/T(\mathbb{Z}^n)$ is finite, and in fact,

$$|\mathbb{Z}^n/T(\mathbb{Z}^n)| = |\det T|.$$

Exercise. Replace $\mathbb{Z}$ by any PID R and formulate and prove the correct analogue of the statement above (in particular, the word "finite" has to be replaced by something else).

Claim 2 (a special case of claim 1). Let $0 \neq v \in A$. Write $r_v : A \to A$ for the map of right multiplication by v, viewed as a homomorphism of $\mathbb{Z}$-modules. Then $|A/Av| = |\det(r_v)|$.

Corollary: If $I \subset A$ is any nonzero left ideal, then $|A/I| < \infty$.

Indeed, if $v \in I$, $v \neq 0$, then $Av \subset I$, so that $|A/I| \leq |A/Av| < \infty$.

$$\alpha \in D \longmapsto r_\alpha \in \mathrm{End}_{\mathbb{Q}}(D)$$

$$\alpha \in A \longmapsto r_\alpha \in \mathrm{End}_{\mathbb{Z}}(A) \cong \mathrm{Mat}_n(\mathbb{Z})$$

Note that $\alpha \longmapsto r_\alpha$ is in fact a ring homomorphism $A^{op} \longrightarrow \mathrm{Mat}_n(\mathbb{Z})$.

Notation. Fix a basis $\omega_1, \dots, \omega_n$ of A as a $\mathbb{Z}$-module, and write $T_i = r_{\omega_i}$ $\forall 1 \le i \le n$.

Dirichlet's pigeon-hole principle

Fix an integer $c \ge 0$, to be chosen later.

Define $Y = \left\{ \sum_{i=1}^{n} m_i \omega_i \;\middle|\; 0 \le m_i \le c \right\} \subset A$

Clearly, $|Y| = (c+1)^n$. Therefore, if $(c+1)^n > |A/I|$, then there exist elements $y_1, y_2 \in Y$ with $y_1 \neq y_2$ and $y_1 \equiv y_2 \bmod I$. That is, if we put $v := y_1 - y_2$, then $0 \neq v \in I$.

It is clear that $v = \sum_{i=1}^{n} m_i \omega_i$ with $\omega_i \in \mathbb{Z}$ and $|\omega_i| \le c$ for all i.

Let us take $c = \lfloor |A/I|^{1/n} \rfloor$ (integral part)

Then $(c+1)^n > |A/I|$, and $c^n \le |A/I|$.

Summing up: we have $0 \neq v \in I$ with $v = \sum_{i=1}^{n} m_i \omega_i$, $|m_i| \leq |A/I|^{1/n}$ $\forall i$.

Now, what is $|A/Av|$? We know:

$$|A/Av| = |\det r_v|, \text{ and by definition,}$$

$$r_v = \sum_{i=1}^{m} m_i \otimes T_i .$$

It is easy to check that $\exists$ constant $L > 0$ s.t.

$$|\det r_v| \leq L \cdot \left(\max\{|m_1|, \ldots, |m_n|\}\right)^n .$$

(Here, L depends only on D, A and probably also $\omega_1, \ldots, \omega_n$. The inequality above only uses the fact that $\det : \mathrm{Mat}_n(\mathbb{Z}) \longrightarrow \mathbb{Z}$ is a homogeneous polynomial of degree n.)

So: $$|A/Av| \leq L \cdot |A/I|$$

$$\Longleftrightarrow \quad |I/Av| \leq L .$$

This completes the proof of the proposition. //.

Next time: the unit theorem.