Goal: Class Field Theory

What type of questions does one want to answer?

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

\[
f(x) = a x^d + b x^{d-1} + \ldots
\]

Def: A prime number \( p \) is split for \( f(x) \)

if \( p \not| a \) and \( \overline{f}(x) = \overline{a} \cdot \prod_{i=1}^{d} (x - x_i) \) in \( \mathbb{F}_p[x] \),

where \( \overline{a} \) is the residue class of \( a \) mod \( p \),

and the \( x_i \)'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 \( \exists \ell \in \mathbb{Z} \) s.t. \( \ell^2 \equiv 13 \pmod{p} \).

This is detected by the Legendre symbol:

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

By the Gauss reciprocity law,

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

\( \iff \quad p \equiv \pm 1, \pm 3, \pm 4 \pmod{13} \)

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

Then \( p \) is split for \( f(x) \iff \quad x^n - 1 = \prod_{i=1}^{n} (x - x_i) \text{ in } \mathbb{F}_p[x] \)

where the \( x_i \) 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

\[ R = \text{principal ideal domain (usually } \mathbb{Z} \text{)} \]
\[ K = \text{the fraction field of } R \]
\[ D = \text{finite dimensional division algebra } / K \]

Def: An \underline{\text{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) \( \forall d \in D, \exists \ 0 \neq c \in R \text{ s.t. } c \cdot d \in A \)

\( \Leftrightarrow (\text{i} \iota i) \quad K \otimes_A R \xrightarrow{\sim} D. \)

(iii') \( K \otimes_A R \xrightarrow{\sim} D \quad (\Leftrightarrow (\text{i} \iota i') \quad K \otimes_A R \xrightarrow{\sim} D. \)

Example:

\[ K = \mathbb{Q}, \quad D = \mathbb{Q}(\sqrt{-1}) \]
\[ R = \mathbb{Z}, \quad A = \mathbb{Z}[\sqrt{-1}] \]

More generally:

\[ d \in \mathbb{Z} \setminus \{0\}, \quad D = \mathbb{Q}(\sqrt{d}) \]

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

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 $D = K\omega_1 \oplus \ldots \oplus K\omega_n$ as a $K$-vector space. Write

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

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

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

Therefore $A' = Rc\omega_1 + \ldots + Rc\omega_n$ 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 $D$. \(\blacksquare\)

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

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 \( I_1, I_2 \subseteq A \) are said to be right principal equivalent if there exists \( x \in D \) with \( I_1 x = I_2 \). The set of such equivalence classes is called the class set of \( A \) of nonzero left ideals.

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 \( I_1, I_2 \subseteq A \) are left ideals, then every \( A \)-module homomorphism \( I_1 \rightarrow I_2 \) is given by \( x \mapsto xx \) for some \( x \in D \). 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 \( X = \{ M \subseteq V \mid M \text{ is a finitely generated } A \text{-submodule} \} \). 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 $Iv^{-1} \supset AAv^{-1} = A$, and right multiplication by $v^{-1}$ induces an isomorphism $I/Av \xrightarrow{\sim} Iv^{-1}/A$ 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 $\frac{1}{w}A \subset D$, and $(\frac{1}{w}A)/A$ is finite. i.e. 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 $I \subseteq A$, there exists $\sigma \in I$, $\sigma \neq 0$ with $|\mathbb{A}/\mathbb{A}\sigma| \leq h$.

We begin the proof of this proposition.

Claim 1. Let $T \in \text{Mat}_n(\mathbb{Z})$, $\det(T) \neq 0$. 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 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 $0 \neq \sigma \in A$. Write $r_\sigma : A \rightarrow A$ for the map of right multiplication by $\sigma$, viewed as a homomorphism of $\mathbb{Z}$-modules.

Then $|A/\mathbb{A}\sigma| = |\det(r_\sigma)|$.

Corollary: If $I \subseteq A$ is any non-zero left ideal, then $|A/I| < \infty$.

Indeed, if $\sigma \in I$, $\sigma \neq 0$, then $A\sigma \subseteq I$, so that $|A/I| \leq |A/A\sigma| < \infty$. 
\[ x \in D \quad \mapsto \quad r_x \in \text{End}_\mathbb{Q}(D) \]
\[ x \in A \quad \mapsto \quad r_x \in \text{End}_\mathbb{Z}(A) \cong \text{Mat}_n(\mathbb{Z}) \]

Note that \( x \mapsto r_x \) is in fact a ring homomorphism \( A^{\text{op}} \rightarrow \text{Mat}_n(\mathbb{Z}) \).

**Notation.** Fix a basis \( e_1, \ldots, e_n \) of \( A \) as a \( \mathbb{Z} \)-module, and write \( T_i = r_{e_i} \quad \forall 1 \leq i \leq n \).

**Dirichlet's pigeon-hole principle**

Fix an integer \( c > 0 \) to be chosen later.

Define \( Y = \left\{ \sum_{i=1}^{n} m_i e_i \mid 0 \leq m_i \leq c \right\} \subset A \)

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 \( y_1, y_2 \in Y \) with \( y_1 \neq y_2 \) mod \( I \). That is, if we put \( \nu := y_1 - y_2 \), then \( 0 \neq \nu \in I \).

It is clear that \( \nu = \sum_{i=1}^{n} m_i e_i \) with \( m_i \in \mathbb{Z} \) and \( |m_i| \leq c \) for all \( i \).

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

Then \( (c+1)^n > |A/I| \), and \( c^n \leq |A/I| \).
Summing up: we have $0 \neq v \in \mathbb{I}$ 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:

$$|A/Av| = |\det r_v|,$$

and by definition,

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

It is easy to check that there exists a constant $L > 0$ such that

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

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

So:

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

$$\Rightarrow |I/Av| \leq L.$$

This completes the proof of the proposition.

Next time: the unit theorem.