Lecture Notes to a Course on Algebraic Number Theory

Taught by Prof. Uri Shapira at Technion IIT during Spring 2022

Typed by Elad Tzorani

March 20, 2022

Course Information

The course will be based on lecture notes by Ehud De Shalit on algebraic number theory, and partially on Milne's text on algebraic number theory (henceforward, ANT).

Prerequisites

The course will assume undergraduate knowledge in ring theory and Galois theory.

1 Notations & Conventions

- All rings are assumed to be commutative and unital, unless mentioned otherwise.
- The rings of integers, reals and complex numbers are respectively denoted $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$.
- For $n \in \mathbb{Z}_+$ we denote $[n] = \{1, \ldots, n\}$.

2 A Short Review on Rings

Definition 2.1 (Euclidean Ring)**.** Let R be a ring. We say R is *Euclidean* if there is a map $N \colon R \to \mathbb{Z}_+$ that satisfies the following properties.

(i) *Sub-multiplicativity:* $N(a) = 0$ if and only if $a = 0$, and
$$N(\alpha\beta) \leq N(\alpha) N(\beta).$$

(ii) For all $\alpha, \beta \in R$ such that $\alpha \neq 0$, there are $q, r \in R$ such that
$$\beta = q\alpha + r, \quad N(r) < N(\alpha).$$

Such a map is called the *Euclidean norm* of R.

Definition 2.2 (Group of Units in a Ring)**.** Let R be a ring. The *group of units* in R is

$$R^{\times} \coloneqq \{\alpha \in R \mid \exists \beta \in R \colon \alpha\beta = 1\}.$$

Definition 2.3 (Associate Elements)**.** Let R be a ring and let $\alpha, \beta \in R$. We say that α, β are *associates*, and denote $\alpha \sim \beta$, if there's $\varepsilon \in R^{\times}$ such that $\alpha = \varepsilon\beta$.

Definition 2.4 (Reducible Element)**.** Let R be a ring and let $\alpha \in R \setminus \{0\}$. We say that α is *reducible* if there are $\beta, \gamma \in R \setminus R^{\times}$ such that $\alpha = \beta \cdot \gamma$.

Remark 2.5. The subset of reducible elements of R is $R^{\times} \cdot R^{\times}$.

Definition 2.6 (Irreducible Element)**.** Let R be a ring. An element $\alpha \in R$ is *irreducible* if it isn't reducible.

Definition 2.7 (Prime Elements)**.** Let R be a ring and let $\alpha \in R \setminus (R^{\times} \cup \{0\})$. We say that α is *prime* if for $\beta, \gamma \in R$ such that $\alpha \mid \beta \cdot \gamma$ one has either $\alpha \mid \beta$ or $\alpha \mid \gamma$.

Definition 2.8 (Ideal in a Ring)**.** Let R be a ring. An *ideal* of R is a strict non-zero subset $I \subseteq R$ that is an additive subgroup and such that $aI, Ia \subseteq I$ for all $a \in R$.

Notation 2.9. Let R be a ring. We denote $I \leq R$ to say that I is an ideal of R.

Definition 2.10 (Prime Ideal)**.** Let R be a ring and let $I \leq R$. We say that I is *prime* if whenever $\beta, \gamma \in R$ are such that $\beta \cdot \gamma \in I$, one has $\beta \in I$ or $\gamma \in I$.

Definition 2.11 (Principal Ideal)**.** Let R be a ring and let $\alpha \in R$. We denote

$$(\alpha) \coloneqq \alpha \cdot R = \{\alpha \cdot \beta \mid \beta \in R\}.$$

Ideals of this form are called *principal ideals*.

Definition 2.12. Let R be a ring. We say that R is a *principal ideal domain (PID)* if any ideal of R is principal.

Theorem 2.13. *Any Euclidean domain is PID.*

Lemma 2.14. *Let R be a ring and let $\alpha \in R$. Then α is prime if and only if (α) is a prime ideal.*

Lemma 2.15. *Let R be a ring. Prime elements of R are irreducible.*

Exercise 2.1. Let R be a ring and let $I \leq R$. Then I is prime if and only if R/I is an integral domain.

Exercise 2.2. Let R be a ring. An ideal $I \leq R$ is maximal if and only if R/I is a field.

Corollary 2.16. *Maximal ideals are prime.*

Exercise 2.3. Let R be a ring and let $\alpha \in R$. Then α is irreducible if and only if (α) is maximal among principal ideals.

Definition 2.17 (Unique Factorization Domain)**.** Let R be a ring. We say that R is a *unique factorization domain (UFD)* if any $\alpha \in R$ can be written as $\alpha = \beta_1 \cdot \ldots \cdot \beta_k$ where $\beta_i \in R$ are irreducible, and if $\beta_1 \cdot \ldots \cdot \beta_k = \gamma_1 \cdot \ldots \cdot \gamma_\ell$ are two products of irreducible elements of R, then $\ell = k$ and there is a bijection $\sigma \colon [k] \to [k]$ such that $\beta_i \sim \gamma_{\sigma(i)}$.

Corollary 2.18. *Let R be a PID or a UFD. Any irreducible ideal of R is prime.*

Exercise 2.4. A PID is also a UFD.

Example 2.19. Consider the ring $R \coloneqq \mathbb{Z}\left[\sqrt{-5}\right]$. We can write

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

which are two possible decompositions of 6 in $\mathbb{Z}\left[\sqrt{-5}\right]$. We claim that $2, 3, \left(1 + \sqrt{-5}\right), \left(1 + \sqrt{-5}\right)$ are all irreducible and non-associates, which implies that $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD.

On R we have a multiplicative *norm* map (that doesn't make it an Euclidean domain)

$$\begin{aligned} N \colon \mathbb{Z}\left[\sqrt{-5}\right] &\to \mathbb{Z} \\ a + b\sqrt{-5} &\mapsto \left(a + b\sqrt{-5}\right)\left(a - b\sqrt{-5}\right) = a^2 + 5b^2. \end{aligned}$$

One can use N to check that $2, 3, \left(1 + \sqrt{-5}\right), \left(1 + \sqrt{-5}\right)$ are irreducible and non-associates.

Exercise 2.5. Use N to check that $2, 3, \left(1 + \sqrt{-5}\right), \left(1 + \sqrt{-5}\right)$ are irreducible and non-associates.

3 Preliminaries to Algebraic Number Theory

3.1 Definition and Motivation

ANT is the study of finite field extensions of $\mathbb{Q}$ and their rings of integers. ANT is used in solving and analysis of questions about integers.

Definition 3.1 (Number Field)**.** A field K is called a *number field* if $\mathbb{Q} \subseteq K$ and

$$[K : \mathbb{Q}] \coloneqq \deg\left(K/\mathbb{Q}\right) < \infty.$$

Definition 3.2 (p-Adic Valuation)**.** Let $n \in \mathbb{Z}$ and let $p \in \mathbb{Z}$ be a prime. For $n \neq 0$, we denote by $v_p(n)$ the power in which p appears in the decomposition of n into primes; we denote also $v_p(0) = \infty$. We call $v_p \colon \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ the *p-adic valuation.*

Theorem 3.3 (Fermat)**.** *An integer $n \in \mathbb{Z}$ is a sum of two squares if and only if for any $q \in \mathbb{Z}$ satisfying $q \equiv 3 \pmod 4$ one has $v_q(n) \in 2\mathbb{Z}$.*

Proof. Consider the ring $R = \mathbb{Z}[i]$ of *Gaussian integers* and the *norm*

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{Z} \\ a+bi &\mapsto (a+bi)(a-bi) = a^2+b^2. \end{aligned}$$

- We first claim that R is an Euclidean domain. We show this by showing that N is an Euclidean norm. Let $\alpha, \beta \in R$ with $\alpha \neq 0$. We want to find $q, r \in \mathbb{Z}[i]$ such that $N(r) < N(\alpha)$ and $\beta = q\alpha + r$. Write $\beta = \beta/\alpha \cdot \alpha$ in $\mathbb{Q}[i] = \mathrm{Frac}(R)$. For any $q \in \mathbb{Z}[i]$ we can write

  $$\begin{aligned} \beta &= \alpha + \frac{\beta}{\alpha} \cdot \alpha - q \cdot \alpha \\ &= q \cdot \alpha + \alpha \left(\frac{\beta}{\alpha} - q \right). \end{aligned}$$

  Extend $N\colon \mathbb{Q}(i) \to \mathbb{Q}$ via $N(a+bi) = a^2+b^2$. We show that there's $q \in \mathbb{Z}[i]$ such that $N(\beta/\alpha - q) < 1$, from which $N(\alpha(\beta/\alpha - q)) < N(\alpha)$ by sub-multiplicativity, as required. Indeed, each point of $\mathbb{C}$ is within distance at most 1 from the lattice $\mathbb{Z}[i]$.[1]

- We now show that

  $$\begin{aligned} \mathbb{Z}[i]^\times &= \{\alpha \in \mathbb{Z}[i] \mid N(\alpha \in \{\pm 1\})\} \\ &= \{\pm 1, \pm i\}. \end{aligned}$$

  Let $\alpha \in R$. If $N(\alpha) = \alpha\bar{\alpha} = 1$, we get that $\alpha \in \mathbb{Z}[i]^\times$. On the other hand, if $\alpha \cdot \beta = 1$, we get

  $$N(\alpha) N(\beta) = N(\alpha\beta) = N(1) = 1$$

  so $N(\alpha) \in \mathbb{Z}^\times$ so $N(\alpha) \in \{\pm 1\}$. [2]

- We want to understand

  $$\mathrm{im}(N) = \{N(z) = z\bar{z} \mid z \in \mathbb{Z}\} = \left\{a^2+b^2 \;\middle|\; a, b \in \mathbb{Z}\right\}.$$

  - Let p be a *rational prime* (i.e. prime in $\mathbb{Z}$. We have

    $$\begin{aligned} \mathbb{Z}[i]/(p) &\cong \mathbb{Z}[x]/\left(x^2+1, p\right) \\ &\cong \mathbb{F}_p[x] \end{aligned}$$

    so p remains a prime in $\mathbb{Z}[i]$ if and only if -1 is not a square in $\mathbb{F}_p$.

[1] We say that the *covering radius* of $\mathbb{Z}[i] \subseteq \mathbb{C}$ is $\sqrt{2}/2$, since this is the smallest number for which any ball in $\mathbb{C}$ of radius r contains a point of $\mathbb{Z}](i)$.

[2] Note that in our case, $N(\alpha) \geq 0$ so it follows that $N(\alpha) = 1$. The statement is more general when one requires $N(\alpha) \in \{\pm 1\}$ instead.

- We claim that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. From this and the above calculation we get that p remains a prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$.

  Consider

  $$\begin{aligned} \varphi \colon \mathbb{F}_p^\times &\to \mathbb{F}_p^\times \\ \alpha &\mapsto \alpha^2. \end{aligned}$$

  We have $\ker(\varphi) = \{\pm 1\}$, so by the isomorphism theorem $\operatorname{im}(\varphi)$ is a subgroup of $\mathbb{F}_p^\times$ of size $\#\mathbb{F}_p / \#\{\pm 1\} = \frac{p-1}{2}$. We get that $-1 \in \operatorname{im}(\varphi)$ if and only if $\ker(\varphi)|_{\operatorname{im}(\varphi)} \neq \{1\}$. Now, $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ and $\operatorname{im}(\varphi) \subseteq \mathbb{F}_p^\times$ is another cyclic group of size $\frac{p-1}{2}$; hence this is the case when 2 and $\frac{p-1}{2}$ are coprime, or equivalently $p \equiv 1 \pmod 4$.

- Note that $2 = (1+i)(1-i)$, where $1 \pm i$ are irreducible because $N(1+i)$ is prime in $\mathbb{Z}$. Hence this is a decomposition of 2 into a product of irreducible elements and in particular 2 isn't prime in $\mathbb{Z}[i]$. (**Exercise:** Write formally why $1 \pm i$ are irreducible elements of $\mathbb{Z}[i]$.)

- If $p \equiv 1 \pmod 4$ is a rational prime, we claim that there's an irreducible element $\pi \in \mathbb{Z}[i]$ for which $p = \pi\bar{\pi}$ and $N(\pi) = p$.

  To show this, write $p = \pi\lambda$ for π irreducible and λ non-unit. We get

  $$\begin{aligned} p^2 &= N(p) \\ &= N(\pi) \cdot N(\lambda) \\ &= \pi\bar{\pi} \cdot \lambda\bar{\lambda}. \end{aligned}$$

  Since λ is a non-unit, we get $\lambda\bar{\lambda} \neq 1$, so $\lambda\bar{\lambda} \in \{p, p^2\}$. Similarly, $\pi\bar{\pi} \in \{p, p^2\}$, hence $\pi\bar{\pi} = \lambda\bar{\lambda} = p$, as required.

- We claim that if $\pi \in \mathbb{Z}[i]$ is an irreducible element other than $1 \pm i$ and not in $\mathbb{Z}$, then $pcoloneqq\pi\bar{\pi}$ is a rational prime with $p \equiv 1 \pmod 4$.

  Indeed, consider $p \coloneqq N(\pi) = \pi\bar{\pi}$ is a product of rational primes. By the uniqueness of the decomposition it follows that $p \equiv 1 \pmod 4$ is a rational prime.

In conclusion, taking $z \in \mathbb{Z}[i]$ we can write

$$z = \varepsilon (1+i)^r \left(\prod_{i \in [k]} \pi_i^{m_i} \right) \left(\prod_{j \in [\ell]} q_j^{n_j} \right)$$

for $\varepsilon \in \mathbb{Z}[i]$ a unit, π_i primes in $\mathbb{Z}[i]$ of norms p_i which are rational primes with $p_i \equiv 1 \pmod 4$, and q_j are rational primes with $q_j \equiv 3 \pmod 4$. We get that

$$N(z) = 2^r \left(\prod_{i \in [k]} p_i^{m_i} \right) \left(\prod_{j \in [\ell]} q_j^{2m_j} \right).$$

From here one gets the result.

$\square$

3.2 Field Embeddings

Definition 3.4 (Field Embedding)**.** Let K, L be two fields. Field homomorphisms $\sigma \colon K \to L$ are called *field embeddings.* The collection of such embeddings is denoted $\mathrm{Emb}\,(K, L)$.

Definition 3.5 (Real & Complex Embeddings)**.** An embedding $\sigma \in \mathrm{Emb}\,(K, \mathbb{C})$ is called *real* if $\sigma\,(K) \subseteq \mathbb{R}$. It is called *complex* otherwise.

Theorem 3.6. *Let K be a degree n number field. There are exactly n distinct embeddings $\sigma_i \colon K \to \mathbb{C}$.*

Corollary 3.7. *Let K be an algebraic number field of degree n. There are $r_1, r_2 \in \mathbb{Z}$ non-negative with r_1 real embeddings and $2r_2$ complex embeddings which are divided into pairs of the form $\sigma, \bar{\sigma}$. We have $n = r_1 + 2r_2$.*

We fix an ordering of $\mathrm{Emb}\,(K, \mathbb{C})$*:*

$$\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \ldots, \sigma_{r_1+2r_2}$$

such that $\sigma_{r_1+1}, \ldots, \sigma_{r_1}$ are real embeddings, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ are non-conjugate complex embeddings, and for all $i \in [r_2]$ one has $\bar{\sigma}_{r_1+r_2+j} = \sigma_{r_1+j}$.

Definition 3.8 (Geometric Embedding of a Field into $\mathbb{R}^n$)**.** Let K be an algebraic number field of degree n. Let r_1, r_2 be as in the above corollary. We define a $\mathbb{Q}$-linear map

$$\begin{aligned} &\varphi \colon K \to \mathbb{R}^n \cong \mathbb{R}^{r_1} \times \left(\mathbb{R}^2\right)^{r_2} \\ &\quad \alpha \mapsto \left(\sigma_1\left(\alpha\right), \sigma_2\left(\alpha\right), \ldots, \sigma_{r_1}\left(\alpha\right), \Re\left(\sigma_{r_1+1}\left(\alpha\right)\right), \Im\left(\sigma_{r_1+1}\left(\alpha\right)\right), \ldots, \Re\left(\sigma_{r_1+r_2}\left(\alpha\right)\right), \Im\left(\sigma_{r_1+r_2}\left(\alpha\right)\right)\right). \end{aligned}$$

This is called the *geometric embedding of K into $\mathbb{R}^n$.*

Proposition 3.9. *Let K be an algebraic number field of degree n, and let φ be as above. Then $\varphi\,(K)$ contains an $\mathbb{R}$-basis of $\mathbb{R}^n$.*