0.1. Prerequisites

- **Definition**: $I \subset R$ is **prime ideal** if $\forall a, b \in R, ab \in I \Longrightarrow a \in I \vee b \in I$.
- **Definition**: ideal I is **maximal** if $I \neq R$ and there is no ideal $J \subset R$ such that $I \subset J$.
- **Example**:
  - $p \in \mathbb{Z}$ is prime iff $\langle p \rangle = p\mathbb{Z}$ is prime ideal.
  - $\langle 0 \rangle$ is prime ideal iff R is integral domain.
- **Lemma**: if I is maximal ideal, then it is prime.
- **Proposition**: for commutative ring R, ideal I:
  - $I \subset R$ is prime ideal iff R/I is an integral domain.
  - I is maximal iff R/I is field.
- **Proposition**: let R be PID and $a \in R$ irreducible. Then $\langle a \rangle = \langle a \rangle_R$ is maximal.
- **Theorem**: let F be field, $f(x) \in F[x]$ irreducible. Then $F[x]/\langle f(x) \rangle$ is a field and a vector space over F with basis $B = \{1, \overline{x}, ..., \overline{x}^{n-1}\}$ where $n = \deg(f)$. That is, every element in $F[x]/\langle f(x) \rangle$ can be uniquely written as linear combination

$$\overline{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}}, \quad a_i \in F$$

1. Divisibility in rings

1.1. Every ED is a PID

- **Definition**: let R integral domain. $\varphi : R - \{0\} \to \mathbb{N}_0$ is **Euclidean function (norm)** on R if:
  - $\forall x, y \in R - \{0\}, \varphi(x) \leq \varphi(xy)$.
  - $\forall x \in R, y \in R - \{0\}, \exists q, r \in R : x = qy + r$ with either $r = 0$ or $\varphi(r) < \varphi(y)$.

  R is **Euclidan domain (ED)** if Euclidean function is defined on it.
- **Example**:
  - $\mathbb{Z}$ is ED with $\varphi(n) = |n|$.
  - $F[x]$ is ED for field F with $\varphi(f) = \deg(f)$.
- **Lemma**: $\mathbb{Z}[-\sqrt{2}]$ is ED with Euclidean function

$$\varphi(a + b\sqrt{-2}) = N(a + b\sqrt{-2}) =: a^2 + 2b^2$$

- **Proposition**: every ED is a PID.

1.2. Every PID is a UFD

- **Definition**: Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit in R can be written uniquely (up to order of factors and multiplication by units) as product of irreducible elements in R.
- **Example**: let $R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$. Its units are ± 1. Any factorisation of $x \in R$ must be of the form $f(x)g(x)$ where $\deg f = 1, \deg g = 0$, so $x = (ax + b)c$, $a \in \mathbb{Q}$, $b, c \in \mathbb{Z}$. We have $bc = 0$ and $ac = 1$ hence $x = \frac{x}{c} \cdot c$. So x irreducible if $c \neq \pm 1$. Also, any factorisation of $\frac{x}{c}$ in R is of the form $\frac{x}{c} = \frac{x}{cd} \cdot d$, $d \in \mathbb{Z}$, $d \neq 0$. Again, neither factor is a unit when $d \neq \pm 1$. So $x = \frac{x}{c} \cdot c = \frac{x}{cd} \cdot c \cdot c = \cdots$ can never be decomposed into irreducibles (the first factor is never irreducible).

- **Lemma**: let R be PID. Then every irreducible element is prime in R.
- **Theorem**: every PID is a UFD.
- **Example**: $\mathbb{Z}\left[\sqrt{-2}\right]$ so by the above theorem it is a UFD. Let $x, y \in \mathbb{Z}$ such that $y^2 + 2 = x^3$.
  - y must be odd, since if $y = 2a, a \in \mathbb{Z}$ then $x = 2b, b \in \mathbb{Z}$ but then $2a^2 + 1 = 4b^3$.
  - $y \pm \sqrt{-2}$ are relatively prime: if $a + b\sqrt{-2}$ divides both, then it divides their difference $2\sqrt{-2}$, so norm $a^2 + 2b^2 \mid N\left(2\sqrt{-2}\right) = 8$. Only possible case is $a = \pm 1, b = 0$ so $a + b\sqrt{-2}$ is unit. Other cases $a = 0, b = \pm 1$, $a = \pm 2, b = 0$ and $a = 0, b = \pm 2$ are impossible since y not even.
  - If $a + b\sqrt{-2}$ is unit, $\exists x, y \in \mathbb{Z} : \left(a + b\sqrt{-2}\right)\left(x + y\sqrt{-2}\right) = 1$. If $b \neq 0$ then $(-a^2 - 2b^2)y = 1 \Longrightarrow b = 0$: contradiction. If $b = 0$, $a = \pm 1$.

2. Finite field extensions

- **Definition**: let F, L fields. If $F \subseteq L$ and F and L share the same operations then F is a **subfield** of L and L is **field extension** of F (denoted L/F). L is vector space over F:
  - $0 \in L$ (zero vector).
  - $u, v \in L \Longrightarrow u + v \in L$ (additivity).
  - $a \in F, u \in L \Longrightarrow au \in L$ (scalar multiplication).
- **Definition**: let L/F field extension. **Degree** of L over F is dimension of L as vector space over F:

$$[L : F] := \dim_F(L)$$

  If $[L : F]$ finite, L/F is **finite field extension**.
- **Example**: $\mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} : a, b \in \mathbb{Q}\}$ is isomorphic as a vector space to $\mathbb{Q}^2$ so is 2-dimensional vector space over $\mathbb{Q}$. Isomorphism is $a + b\sqrt{-2} \longleftrightarrow (a, b)$. Standard basis $\{e_1, e_2\}$ in $\mathbb{Q}^2$ corresponds to the basis $\{1, \sqrt{-2}\}$ in $\mathbb{Q}(\sqrt{-2})$. $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$.
- **Example**: $[\mathbb{C} : \mathbb{R}] = 2$ (a basis is $\{1, i\}$). $[\mathbb{R} : \mathbb{Q}]$ is not finite, due to the existence of transcendental numbers (if α transcendental, then $\{1, \alpha, \alpha^2, ...\}$ is linearly independent).
- **Definition**: let L/F field extension. $\alpha \in L$ is **algebraic** over F if

$$\exists f(x) \in F[x] : f(\alpha) = 0$$

  If all elements in L are algebraic, then L/F is **algebraic field extension**.
- **Example**: $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ since i is root of $x^2 + 1$. $\mathbb{C}/\mathbb{R}$ is algebraic since $z = a + bi$ is root of $(x - z)(x - \overline{z}) = x^2 - 2ax + a^2 + b^2$.
- **Proposition**: if L/F is finite field extension then it is algebraic.
- **Definition**: let L/F field extension, $\alpha \in L$ algebraic over F. **Minimal polynomial** $p_\alpha(x) = p_{\alpha,F}(x)$ of α over F is the monic polynomial f of smallest degree such that $f(\alpha) = 0$. **Degree** of α over F is $\deg(p_\alpha)$.
- **Proposition**: $p_\alpha(x)$ is unique and irreducible. Also, if $f(x) \in F[x]$ is monic, irreducible and $f(\alpha) = 0$, then $f = p_\alpha$.

- **Example**:
  - $p_{i,\mathbb{R}}(x) = p_{i,\mathbb{Q}}(x) = x^2 + 1$, $p_{i,\mathbb{Q}(i)}(x) = x - i$.
  - Let $\alpha = \sqrt[7]{5}$. $f(x) = x^7 - 5$ is minimal polynomial of α over $\mathbb{Q}$, as it is irreducible by Eisenstein's criterion with $p = 5$ and the above proposition.
  - Let $\alpha = e^{2\pi i/p}$, p prime. α is algebraic as root of $x^p - 1$ which isn't irreducible as $x^p - 1 = (x-1)\Phi(x)$ where $\Phi(x) = (x^{p-1} + \cdots + 1)$. $\Phi(\alpha) = 0$ since $\alpha \neq 1$, $\Phi(x)$ is monic and $\Phi(x+1) = ((x+1)^p - 1)/x$ irreducible by Eisenstein's criterion with $p = p$, hence $\Phi(x)$ irreducible. So $p_\alpha(x) = \Phi(x)$.

2.1. Fields generated by elements

- **Definition**: let L/F field extension, $\alpha \in L$. The **field generated by α over F** is the smallest subfield of L containing F and α:

$$F(\alpha) := \bigcap_{\substack{K \text{ field}, \\ F \subseteq K \subseteq L, \\ \alpha \in K}} K$$

  Generally, $F(\alpha_1, ..., \alpha_n)$ is smallest field extension of F containing $\alpha_1, ..., \alpha_n$.
- We have $F(\alpha_1, ..., \alpha_n) = F(\alpha_1) \cdots (\alpha_n)$ (show $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$ and $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$ by minimality and use induction).
- **Definition**: $F[\alpha] = \{\sum_{i=0}^n a_i \alpha^i : a_i \in F, n \in \mathbb{N}\} = \{f(\alpha) : f(x) \in F[x]\}$.
- **Lemma**: let L/F field extension, $\alpha \in L$ algebraic over F. Then $F[\alpha]$ is field, hence $F(\alpha) = F[\alpha]$.
- **Lemma**: let α algebraic over F. Then $[F(\alpha) : F] = \deg(p_\alpha)$.
- **Definition**: let K/F and L/K field extensions, then $F \subseteq K \subseteq L$ is **tower of fields**.
- **Tower theorem**: let $F \subseteq K \subseteq L$ tower of fields. Then

$$[L : F] = [L : K] \cdot [K : F]$$

- **Example**: let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Show $[L : \mathbb{Q}] = 4$.
  - Let $K = \mathbb{Q}(\sqrt{2})$. Let $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ so $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. So $0 \in \{a, b\}$, otherwise $\sqrt{2} \in \mathbb{Q}$. But if $a = 0$, then $\sqrt{6} = 2b \in \mathbb{Q}$, if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$: contradiction. So $x^2 - 3$ has no roots in K so is irreducible over K so $p_{\sqrt{3},K}(x) = x^2 - 3$.
  - So $[L : K] = 2$ so by the tower theorem, $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 4$.

2.2. Norm and trace

- Let L/F finite field extension, $n = [L : F]$. For any $\alpha \in L$, there is F-linear map

$$\hat{\alpha} : L \longrightarrow L, \quad x \mapsto \alpha x$$

- With basis $\{\alpha_1, ..., \alpha_n\}$ of L over F, let $T_\alpha = T_{\alpha,L/F} \in M_n(F)$ be the corresponding matrix of the linear map α with respect to the basis $\{\alpha_i\}$:

$$\begin{aligned} \hat{\alpha}(\alpha_1) &= \alpha\alpha_1 = a_{1,1}\alpha_1 + \cdots + a_{1,n}\alpha_n, \\ &\vdots \\ \hat{\alpha}(\alpha_n) &= \alpha\alpha_n = a_{n,1}\alpha_1 + \cdots + \alpha_{n,n}\alpha_n \end{aligned}$$

with $a_{i,j} \in F$, $T_\alpha = (a_{i,j})$, so α is eigenvalue of T_α:

$$\alpha \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = T_\alpha \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

- **Definition**: **norm** of α is

$$N_{L/F}(\alpha) := \det(T_\alpha)$$

- **Definition**: **trace** of α is

$$\operatorname{tr}_{L/F}(\alpha) := \operatorname{tr}(T_\alpha)$$

- **Remark**: norm and trace are independent of choice of basis so are well-defined (uniquely determined by α).
- **Example**: let $L = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ non-square, let $\alpha = a + b\sqrt{m} \in L$. Fix basis $\{1, \sqrt{m}\}$. Now

$$\begin{aligned} \hat{\alpha}(1) &= \alpha \cdot 1 = a + b\sqrt{m}, \\ \hat{\alpha}(\sqrt{m}) &= \alpha\sqrt{m} = bm + a\sqrt{m}, \\ T_\alpha &= \begin{bmatrix} a & b \\ bm & a \end{bmatrix} \end{aligned}$$

So $N_{L/F}(\alpha) = a^2 - b^2 m$, $\operatorname{tr}_{L/F}(\alpha) = 2a$.
- **Lemma**: the map $L \to M_n(F)$ given by $\alpha \mapsto T_\alpha$ is injective ring homomorphism. So if $f(x) \in F[x]$,

$$T_{f(\alpha)} = f(T_\alpha)$$

($f(T_\alpha)$ is a polynomial in T_α, not f applied to each entry).
- **Proposition**: let L/F finite field extension. $\forall \alpha, \beta \in L$,
  - $N_{L/F}(\alpha) = 0 \Longleftrightarrow \alpha = 0$.
  - $N_{L/F}(\alpha\beta) = N_{L/F}(\alpha) N_{L/F}(\beta)$.
  - $\forall a \in F, N_{L/F}(a) = a^{[L:F]}$ and $\operatorname{tr}_{L/F}(a) = [L : F]\alpha$.
  - $\forall a, b \in F, \operatorname{tr}_{L/F}(a\alpha + b\beta) = a \operatorname{tr}_{L/F}(\alpha) + b \operatorname{tr}_{L/F}(\beta)$ (so $\operatorname{tr}_{L/F}$ is F-linear map).

2.3. Characteristic polynomials

- Let $A \in M_n(F)$, then characteristic polynomial is $\chi_A(x) = \det(xI - A) \in F[x]$ and is monic, $\deg(\chi_A) = n$. If $\chi_A(x) = x^n + \sum_{i=0}^{n=1} c_i x^i$ then $\det(A) = (-1)^n \det(0 - A) = (-1)^n \chi_A(0) = (-1)^n c_0$ and $\operatorname{tr}(A) = -c_{n-1}$, since if $\alpha_1, ..., \alpha_n$ are eigenvalues of A (in some field extension of F), then $\operatorname{tr}(A) = \alpha_1 + \cdots + \alpha_n$, $\chi_A(x) = (x - \alpha_1) \cdots (x - \alpha_n) = x^n - (\alpha_1 + \cdots \alpha_n) x^{n-1} + \cdots$.
- For finite extension L/F, $n = [L : F]$, $\alpha \in L$, **characteristic polynomial** $\chi_\alpha(x) = \chi_{\alpha,L/F}(x)$ is characteristic polynomial of T_α. So $N_{L/F}(\alpha) = (-1)^n c_0$, $\operatorname{tr}_{L/F}(\alpha) = -c_{n-1}$. By the Cayley-Hamilton theorem, $\chi_\alpha(T_\alpha) = 0$ so $T_{\chi_\alpha(\alpha)} = \chi_\alpha(T_\alpha) = 0$, where $\chi_\alpha(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_0$. Since $\alpha \to T_\alpha$ is injective, $\chi_\alpha(\alpha) = 0$.

- **Lemma**: let L/F finite extension, $\alpha \in L$ with $L = F(\alpha)$. Then $\chi_\alpha(x) = p_\alpha(x)$.
- **Proposition**: let $F \subseteq F(\alpha) \subseteq L$, let $m = [L : F(\alpha)]$. Then $\chi_\alpha(x) = p_\alpha(x)^m$.
- **Corollary**: let L/F, $\alpha \in L$ as above, $p_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, $a_i \in F$. Then

$$N_{L/F}(\alpha) = (-1)^{md} a_0^m, \quad \mathrm{tr}_{L/F}(\alpha) = -m a_{d-1}$$

3. Algebraic number fields and algebraic integers

3.1. Algebraic numbers

- **Definition**: $\alpha \in \mathbb{C}$ is **algebraic number** if algebraic over $\mathbb{Q}$.
- **Definition**: K is **(algebraic) number field** if $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ and $[K : \mathbb{Q}] < \infty$.
- Every element of an algebraic number field is an algebraic number.
- **Example**: let $\theta = \sqrt{2} + \sqrt{3}$, then $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ but also $\theta^3 = 11\sqrt{2} + 9\sqrt{3}$ so

$$\sqrt{2} = \frac{\theta^3 - 9\theta}{2}, \quad \sqrt{3} = \frac{-\theta^3 + 11\theta}{2}$$

  so $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\theta)$ hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$.
- **Simple extension theorem**: every number field K has form $K = \mathbb{Q}(\theta)$ for some $\theta \in K$.
- Set of all algebraic numbers (union of all number fields) is denoted $\overline{\mathbb{Q}}$ and is a field, since if $\alpha \neq 0$ algebraic over $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(p_\alpha) < \infty$ so $\mathbb{Q}(\alpha)/\mathbb{Q}$ algebraic, so $-\alpha, \alpha^{-1} \in \mathbb{Q}(\alpha)$ algebraic, so $\alpha^{-1}, -\alpha \in \overline{\mathbb{Q}}$, and if $\alpha, \beta \in \overline{\mathbb{Q}}$ then $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)(\beta)$ is finite extension of $\mathbb{Q}$ by tower theorem so $\alpha + \beta$, $\alpha\beta \in \mathbb{Q}(\alpha, \beta)$ so are algebraic.
- $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ since if $[\overline{\mathbb{Q}} : \mathbb{Q}] = d \in \mathbb{N}$ then every algebraic number would have degree $\leq d$, but $\sqrt[d+1]{2}$ has degree $d + 1$ since it is a root of $x^{d+1} - 2$ which is irreducible by Eisenstein's criterion with $p = 2$.
- **Definition**: let $\alpha \in \overline{\mathbb{Q}}$. **Conjugates** of α are roots of $p_\alpha(x)$ in $\mathbb{C}$.
- **Example**:
  - Conjugate of $a + bi \in \mathbb{Q}(i)$ is $a - bi$.
  - Conjugate of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is $a - b\sqrt{2}$.
  - Conjugates of θ do not always lie in $\mathbb{Q}(\theta)$, e.g. for $\theta = \sqrt[3]{2}$, $p_\theta(x) = x^3 - 2$ has two non-real roots not in $\mathbb{Q}(\theta) \subset \mathbb{R}$.
- **Notation**: when base field is $\mathbb{Q}$, N_K and tr_K denote $N_{K/\mathbb{Q}}$ and $\mathrm{tr}_{K/\mathbb{Q}}$.
- **Lemma**: let $K/\mathbb{Q}$ number field, $\alpha \in K$, $\alpha_1, ..., \alpha_n$ conjugates of α. Then

$$N_K(\alpha) = (\alpha_1 \cdots \alpha_n)^{[K:\mathbb{Q}(\alpha)]}, \quad \mathrm{tr}_K(\alpha) = (\alpha_1 + \cdots + \alpha_n)[K : \mathbb{Q}(\alpha)]$$

3.2. Algebraic integers

- **Definition**: $\alpha \in \overline{\mathbb{Q}}$ is **algebraic integer** if it is root of a monic polynomial in $\mathbb{Z}[x]$. The set of algebraic integers is denoted $\overline{\mathbb{Z}}$. If $K/\mathbb{Q}$ is number field, set of algebraic integers in K is denoted $\mathcal{O}_K$, $\alpha \in \mathcal{O}_K$ is called **integer in $\boldsymbol{K}$**.

- **Example**: i, $\left(1+\sqrt{3}\right)/2 \in \overline{\mathbb{Z}}$ since they are roots of x^2+1 and x^2-x+1 respectively.
- **Theorem**: let $\alpha \in \overline{\mathbb{Q}}$. The following are equivalent:
  - $\alpha \in \overline{\mathbb{Z}}$.
  - $p_\alpha(x) \in \mathbb{Z}[x]$.
  - $\mathbb{Z}[\alpha] = \{\sum_{i=0}^{d-1} a_i \alpha^i : a_i \in \mathbb{Z}\}$ where $d = \deg(p_\alpha)$.
  - There exists non-trivial finitely generated abelian additive subgroup $G \subset \mathbb{C}$ such that

$$\alpha G \subseteq G \text{ i.e. } \forall g \in G, \alpha g \in G$$

    (αg is complex multiplication).
- **Remark**:
  - For third statement, generally we have $\mathbb{Z}[\alpha] = \{f(\alpha : f(x) \in \mathbb{Z}[x])\}$ and in this case, $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x], \deg(f) < d\}$.
  - Fourth statement means that

$$G = \{a_1\gamma_1 + \cdots + a_r\gamma_r : a_i \in \mathbb{Z}\} = \gamma_1\mathbb{Z} + \cdots + \gamma_r\mathbb{Z} = \langle \gamma_1, ..., \gamma_r \rangle_{\mathbb{Z}}$$

    G is typically $\mathbb{Z}[\alpha]$. E.g. if $\alpha = \sqrt{2}$, $\mathbb{Z}[\sqrt{2}]$ is generated by $1, \sqrt{2}$ and $\sqrt{2} \cdot \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\sqrt{2}]$.
- **Proposition**: $\overline{\mathbb{Z}}$ is a ring. Also, for every number field K, $\mathcal{O}_K$ is a ring.
- **Lemma**: let $\alpha \in \overline{\mathbb{Z}}$. For every number field K with $\alpha \in K$,

$$N_K(\alpha) \in \mathbb{Z}, \quad \mathrm{tr}_K(\alpha) \in \mathbb{Z}$$

- **Lemma**: let K number field. Then

$$K = \left\{\frac{\alpha}{m} : \alpha \in \mathcal{O}_K, m \in \mathbb{Z}, m \neq 0\right\}$$

- **Lemma**: let $\alpha \in \overline{\mathbb{Z}}$, K number field, $\alpha \in K$. Then

$$\alpha \in \mathcal{O}_K^\times \iff N_K(\alpha) = \pm 1$$

3.3. Quadratic fields and their integers

- **Definition**: $d \in \mathbb{Z}$ is **squarefree** if $d \notin \{0, 1\}$ and there is no prime p such that $p^2 \mid d$.
- **Definition**: $K = \mathbb{Q}(\sqrt{d})$ is a **quadratic field** if d is squarefree. If $d > 0$ then it is **real quadratic**. If $d < 0$ it is **imaginary quadratic**.
- **Proposition**: let $K/\mathbb{Q}$ have degree 2. Then $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}$.
- **Lemma**: let $K = \mathbb{Q}(\sqrt{d})$, $d \equiv 1 \pmod 4$. Then

$$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \left\{\frac{r+s\sqrt{d}}{2} : r, s \in \mathbb{Z}, r \equiv s \pmod 2\right\}$$

- **Theorem**: let $K = \mathbb{Q}(\sqrt{d})$ quadratic field, then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

4. Units in quadratic rings

- **Notation**: in this section, let $K = \mathbb{Q}(\sqrt{d})$ be quadratic number field, $d \in \mathbb{Z} - \{0\}$, $|d|$ is not a square. Let $\mathcal{O}_d = \mathcal{O}_K$. Let $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. The map $x \to \overline{x}$ is a $\mathbb{Q}$-automorphism from K to K.
- **Definition**: S is **quadratic number ring of K** if $S = \mathcal{O}_d$ or $S = \mathbb{Z}[\sqrt{d}]$.
- We have

  $$\alpha \in S^\times \Longrightarrow \exists x \in S : \alpha x = 1 \Longrightarrow N_K(\alpha) N_K(x) = 1 \Longrightarrow N_K(\alpha) = \pm 1$$

  and for $\alpha \in S - \mathbb{Z}$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and so $[K : \mathbb{Q}(\alpha)] = 1$ by the Tower Theorem,

  $$N_K(\alpha) = \pm 1 \Longrightarrow \alpha\overline{\alpha} = \pm 1 \Longrightarrow \alpha \in S^\times$$

  So $\alpha \in S^\times \iff N_K(\alpha) = \pm 1$.
- **Theorem**: to determine the group of units for imaginary quadratic fields:
  -
    - For $d < -1$, $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$.
    - $\mathcal{O}_{-1}^\times = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
  -
    - For $d \equiv 1 \pmod 4$ and $d < -3$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^\times = \{\pm 1\}$.
    - $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = \frac{1+\sqrt{-3}}{2} = e^{\pi i/3}$.
- **Main theorem**: let $d > 1$, d non-square, S be quadratic number ring of $K = \mathbb{Q}(\sqrt{d})$ (i.e. $S = \mathcal{O}_d$ or $S = \mathbb{Z}[\sqrt{d}]$). Then
  - S has a smallest unit $u > 1$ (smaller than all units except 1).
  - $S^\times = \{\pm u^r : r \in \mathbb{Z}\} = \langle -1, u \rangle$.
- **Definition**: the smallest unit $u > 1$ above is the **fundamental unit** of S (or of K, in the case $S = \mathcal{O}_d$).

4.1. Proof of the main theorem

- **Remark**: if $\alpha = a + b\sqrt{d}$ is unit in $\mathbb{Z}[\sqrt{d}]$, $a, b > 0$, then $N_K(\alpha) = \alpha\overline{\alpha} = \pm 1$, so

  $$|\overline{\alpha}| = |a - b\sqrt{d}| = \frac{|N_K(\alpha)|}{|\alpha|} = \frac{1}{|\alpha|} < \frac{1}{b\sqrt{d}} < \frac{1}{b}$$

  Define

  $$A = \left\{\alpha = a + b\sqrt{d} : a, b \in \mathbb{N}_0, |\overline{\alpha}| < \frac{1}{b}\right\}$$

- **Lemma**: $|A| = \infty$.
- **Lemma**: if $\alpha \in A$, then $|N_K(\alpha)| < 1 + 2\sqrt{d}$.
- **Lemma**: $\exists \alpha = a + b\sqrt{d}, \alpha' = a' + b'\sqrt{d} \in A : \alpha > \alpha'$, $|N_K(\alpha)| = |N_K(\alpha')| =: n$ and

$$\alpha \equiv \alpha' \pmod{n}, \quad b \equiv b' \pmod{n}$$

- **Lemma**: there exists a unit u in $\mathbb{Z}[\sqrt{d}]$ such that $u > 1$.
- **Lemma**: let $0 \neq \alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Then $\alpha > \sqrt{|N_K(\alpha)|}$ iff $a, b > 0$.

4.2. Computing fundamental units

- **Theorem**: let $d > 1$ non-square.
  - If $S = \mathbb{Z}[\sqrt{d}]$ and $a + b\sqrt{d} \in S^\times$, $a, b > 0$ such that b is minimal, then $a + b\sqrt{d}$ is the fundamental unit in S.
  - If $S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ (so $d \equiv 1 \pmod{4}$), then
    - $\frac{1+\sqrt{5}}{2}$ is the fundamental unit in $\mathcal{O}_5$.
    - If $d > 5$ and $\frac{s+t\sqrt{d}}{2} \in \mathcal{O}_d^\times$ with $s, t > 0$ such that t is minimal, then $\frac{s+t\sqrt{d}}{2}$ is the fundamental unit in $\mathcal{O}_d$.
- **Remark**: both $u = \frac{1+\sqrt{5}}{2}$ and $u^2 = \frac{3+\sqrt{5}}{2}$ have t minimal (equal to 1), which is why a separate case is needed for $d = 5$.
- **Example**:
  - $1 + \sqrt{2}$ is fundamental unit in $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_2$, since $N_K\left(1 + \sqrt{2}\right) = -1$ so is a unit, and here $b = 1$, so is minimal (as $b > 0$).
  - $2 + \sqrt{5}$ is the fundamental unit in $\mathbb{Z}[\sqrt{5}]$ (since $b = 1$ is minimal) but is not the fundamental unit in $\mathcal{O}_5$.
- **Example**: find fundamental unit in $\mathcal{O}_7$. $7 \not\equiv 1 \pmod{4}$ so $\mathcal{O}_7 = \mathbb{Z}[\sqrt{7}]$. $a + b\sqrt{7}$ is a unit iff $a^2 - 7b^2 = \pm 1$. Also, by the above theorem, it is the fundamental unit if $a, b > 0$ and b is minimal. We use trial and error: for each $b = 1, 2, \ldots$, check whether $7b^2 \pm 1$ is a square

b	$7b^2 - 1$	$7b^2 + 1$	a^2
1	6	8	$-$
2	27	29	$-$
3	62	64	$64 = 8^2$

  So the unit with minimal b such that $a, b > 0$ is $8 + 3\sqrt{7}$, so is the fundamental unit.

4.3. Pell's equation and norm equations

- **Definition**: **Pell's equation** is $x^2 - dy^2 = 1$ for nonsquare d, where solutions are $x, y \in \mathbb{Z}$. Since LHS is norm of $x + y\sqrt{d}$, solutions are given by $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with norm 1.
- **Example**: consider $x^2 - 2y^2 = \pm 1$. Fundamental unit in $\mathbb{Z}[\sqrt{2}]$ is $u = 1 + \sqrt{2}$, with norm -1. So if $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is such that $N_{\mathbb{Z}(\sqrt{2})}\left(x + y\sqrt{2}\right) = 1$, then $x + y\sqrt{2}$ is an even power of u. Thus elements of norm ± 1 are

$$\pm u^{2n} \text{ (RHS} = 1), \quad \pm u^{2n+1} \text{ (RHS} = -1)$$

  To extract solutions x, y, note that if $x + y\sqrt{2} = \pm u^r$, then $x - y\sqrt{2} = \pm \overline{u}^r$, hence

$$x = \pm\frac{u^r + \overline{u}^r}{2}, \quad y = \pm\frac{u^r - \overline{u}^r}{2\sqrt{2}}$$

Solutions when RHS $= 1$ are given by even r, solutions when RHS $= -1$ are given by odd r.

- **Example**: consider $x^2 - 75y^2 = 1$. $75 = 3 \cdot 5^2$ is not square-free, so rewrite as

$$x^2 - 3z^2 = 1$$

where $z = 5y$. Fundamental unit in $\mathbb{Z}[\sqrt{3}]$ is $u = 2 + \sqrt{3}$ of norm 1 so solutions are

$$x = \pm\frac{u^n + \overline{u}^n}{2}, \quad z = \pm\frac{u^n - \overline{u}^n}{2\sqrt{3}}, \quad n \in \mathbb{Z}$$

To get solution for (x, y), we need $5 \mid z$ (which doesn't always hold). Note that

$$u^2 = 7 + 4\sqrt{3} \notin \mathbb{Z}[\sqrt{75}] = \mathbb{Z}[5\sqrt{3}], \quad u^3 = 26 + 3\sqrt{75} \in \mathbb{Z}[\sqrt{75}]$$

Thus when $n = 2$, (x, z) is not solution, but is when $n = 3$, and hence when $n = 3k$ for $k \in \mathbb{Z}$:

$$x = \pm\frac{u^{3k} + \overline{u}^{3k}}{2}, \quad y = \pm\frac{u^{3k} - \overline{u}^{3k}}{5 \cdot 2\sqrt{3}}, \quad k \in \mathbb{Z}$$

u^{3k+1} and u^{3k+2} never give solutions, since if $u^{3k+1} \in \mathbb{Z}[\sqrt{75}]$, then $u \in \mathbb{Z}[\sqrt{75}]$ (since $u^{-3k} \in \mathbb{Z}[\sqrt{75}]$). Similarly, if $u^{3k+2} \in \mathbb{Z}[\sqrt{75}]$, then $u^2 \in \mathbb{Z}[\sqrt{75}]$: contradiction. Note $\mathbb{Z}[\sqrt{75}] \subset \mathbb{Z}[\sqrt{3}]$ and any unit in $\mathbb{Z}[\sqrt{75}]$ is unit in $\mathbb{Z}[\sqrt{3}]$, so is $\pm u^r$ for some $r \in \mathbb{Z}$. So by taking powers of u, eventually we find the fundamental unit in $\mathbb{Z}[\sqrt{75}]$ (as it will be smallest unit > 1 assuming we increment powers from 1).