$\mathcal{O}_K$ is a Dedekind ring

Thm Let $n = [K:\mathbb{Q}] < \infty$. For every ideal $(0) \neq I \subset \mathcal{O}_K$ there exists an ideal $(0) \neq J \subset \mathcal{O}_K$ such that $IJ = (c)$ is principal.

Proof The idea is to prove a special case of the identity

$$\forall f, g \in \mathcal{O}_K[X] \setminus \{0\} \qquad ct(f)\,ct(g) = ct(fg), \qquad (*)$$

where the content $ct(f)$ is the ideal generated by the coefficients of f.

Write $I = (a_0, \dots, a_r)$ and consider $f(X) = a_0 X^r + a_1 X^{r-1} + \cdots + a_r \in \mathcal{O}_K[X]$.

For $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ let $f_i(X) = \sigma_i(a_0)X^r + \cdots + \sigma_i(a_r)$, $f_1 = f$, $g(X) = f_2(X) \cdots f_n(X) \in \mathcal{O}_L[X]$, where $L \subset \mathbb{C}$ is any number field containing all $\sigma_i(K)$. Thm on symmetric functions $\Rightarrow f(X)g(X) \in \mathbb{Z}[X]$.

Each $f_i \in \mathcal{O}_L[X] \Rightarrow g(X) \in \mathcal{O}_L[X]$

$\Rightarrow g(X) \in f(X)g(X) / f(X) \in K[X] \cap \mathcal{O}_L[X] = \mathcal{O}_K[X]$.

Let $c = \gcd(\text{coefficients of } fg) \in \mathbb{Z} \setminus \{0\}$, $J = (b_0, \dots, b_t) \subset \mathcal{O}_K$, where $g(X) = b_0 X^t + \cdots + b_t$. **Claim**: $IJ = c\mathcal{O}_K = (c)$.

(2): $c \in \mathbb{Z}[\{\text{coeff. of } fg\}] \subset \mathbb{Z}[\{a_i b_j\}] \subset IJ \Rightarrow \underline{(c) \subset IJ}$.

(⊆): **Lemma.** Let $\overline{\mathbb{Z}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ integral over } \mathbb{Z}\} = \{\text{algebraic integers}\}$.

(a) If $h(X) = c_0 X^m + \cdots + c_m \in \overline{\mathbb{Z}}[X]$, $c_0 \neq 0$, $h(\alpha) = 0 \Rightarrow h(X)/(X-\alpha) \in \overline{\mathbb{Z}}[X]$

(b) If $h(X) = c_0(X-\alpha_1)\cdots(X-\alpha_m) \in \overline{\mathbb{Z}}[X] \setminus \{0\} \Rightarrow \forall k \le m \quad c_0\alpha_1 \cdots \alpha_k \in \overline{\mathbb{Z}}$.

Cor. If $F(X) = A_0X^r + \cdots + A_r \in \overline{\mathbb{Z}}[X]$, $G(X) \in B_0X^t + \cdots + B_t \in \overline{\mathbb{Z}}[X]$ $(A_0B_0 \neq 0)$, $C \in \overline{\mathbb{Z}}$, $C^{-1}F(X)G(X) \in \overline{\mathbb{Z}}[X] \Rightarrow \forall i,j \quad C^{-1}A_iB_j \in \overline{\mathbb{Z}}$

Lemma $\Rightarrow$ Cor: $F = A_0(X-\alpha_1)\cdots(X-\alpha_r)$, $G = B_0(X-\beta_1)\cdots(X-\beta_t)$, apply (b) to $h(X) = C^{-1}F(X)G(X) \Rightarrow \frac{A_0B_0}{C}\alpha_{i_1}\cdots\alpha_{i_k}\beta_{j_1}\cdots\beta_{j_\ell} \in \overline{\mathbb{Z}}$ $(1 \le i_1 < \cdots < i_k \le r,\ 1 \le j_1 < \cdots < j_\ell \le t)$. But $\pm A_i/A_0$ (resp. $\pm B_j/B_0$) is an elementary symmetric polynomial of $\alpha_1, \dots, \alpha_r$ (resp. $\beta_1, \dots, \beta_t$)

$\Rightarrow \pm \frac{A_iB_j}{C}$ = sum of various $\frac{A_0B_0}{C}\alpha_{i_1}\cdots\alpha_{i_k}\beta_{j_1}\cdots\beta_{j_\ell} \in \overline{\mathbb{Z}}$

Cor (for $F = f$, $G = g$, $C = c$) $\Rightarrow \forall i,j \quad a_ib_j/c \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K \Rightarrow \underline{IJ = (\{a_ib_j\})c \subset (c)}$

therefore $IJ = (c) \Rightarrow$ Thm.

Pf of Lemma (a) $\underline{m=1}$: $h = c_0X + c_1 = c_0(X-\alpha) \Rightarrow h/(X-\alpha) = c_0 \in \overline{\mathbb{Z}}$ $(c_0\alpha \in \overline{\mathbb{Z}})$

$\underline{m>1}$: $h_1(X) = h(X) - c_0X^{m-1}(X-\alpha)$ has $\deg(h_1) < m$, $h_1(\alpha) = 0$, $h_1 \in \overline{\mathbb{Z}}[X]$

Induction: $h_1/(X-\alpha) \in \overline{\mathbb{Z}}[X] \Rightarrow h/(X-\alpha) = c_0X^{m-1} + h_1/(X-\alpha) \in \overline{\mathbb{Z}}[X]$

(b) Applying (a) $m-k$ times $\Rightarrow h_2(X) = h(X)/(X-\alpha_{k+1})\cdots(X-\alpha_m) \in \overline{\mathbb{Z}}[X]$

$\Rightarrow \pm c_0\alpha_1 \cdots \alpha_k = h_2(0) \in \overline{\mathbb{Z}}$.

Divisibility and ideals

Recall: $A = UFD \Rightarrow$ Euclid's lemma holds: $x \in A$ irreducible, $x \mid ab \Rightarrow x \mid a$ or $x \mid b$
($\Leftrightarrow$ $A/(x) = A/xA$ is a domain)

Divisibility and inclusions:

(1) A any ring, $a, b \in A$: $a \mid b \Leftrightarrow b \in Aa = (a) \Leftrightarrow (b) \subset (a) \Leftrightarrow (a) \supset (b)$

(2) A UFD: $(a) \cap (b) = (\operatorname{lcm}(a,b))$

(3) A PID $\Rightarrow$ Bézout property: $\underbrace{(a)+(b)}_{(a,b)} = Aa + Ab = Ad = (d)$, $d = \gcd(a,b)$

Notation for ideals: $a_1, \dots, a_n \in A$ $(a_1, \dots, a_n) = Aa_1 + \dots + Aa_n$ the ideal of A generated by $a_1, \dots, a_n$

In Dedekind rings: divisibility for $(\neq 0)$ ideals satisfies (1):
$I \mid J \Leftrightarrow I \supset J$ (so, if $\alpha \in A \setminus \{0\}$, then: $I \mid (\alpha) \Leftrightarrow \alpha \in I$)
Prime ideals $(\neq 0)$ are then analogues of irreducible elements in UFD's: they satisfy $\underbrace{I \mid (\alpha\beta)}_{\alpha\beta \in I} \Rightarrow \underbrace{I \mid (\alpha)}_{\alpha \in I}$ or $\underbrace{I \mid (\beta)}_{\beta \in I}$

Def. A = any ring. A **prime ideal** of A is an ideal $I \subsetneq A$ such that $[\, ab \in I \Rightarrow a \in I \text{ or } b \in I \,]$ $(a, b \in A)$
$\Updownarrow$
the quotient ring A/I is an integral domain.

Notation: $\operatorname{Spec}(A) = \{ P \mid P \subset A \text{ prime ideal} \}$

Note: $(0) \in \operatorname{Spec}(A) \Leftrightarrow A$ is a domain.

Prop. Let A = domain, $0 \neq x \in A$. (1) $(x) \in \operatorname{Spec}(A) \Rightarrow x$ irreducible.
(2) A UFD, x irreducible $\Rightarrow (x) \in \operatorname{Spec}(A)$.
(3) A PID, " .

Pf: (1) $0 \neq x \neq$ irreducible $\Rightarrow$ $\left.\begin{cases} x \in A^* \Rightarrow (x) = A \\ x = ab,\ a, b \notin A^* \Rightarrow a, b \notin (x) \end{cases}\right\} \Rightarrow (x) \notin \operatorname{Spec}(A)$

(2) True by uniqueness of factorisation.
(3) The proof we gave for A = Euclidean only used Bézout's property.

Ex: K = field $\Rightarrow$ $\operatorname{Spec}(K) = \{(0)\}$

$\operatorname{Spec}(\mathbb{Z}) = \{(0)\} \cup \{(p) \mid p = \text{prime number}\}$

$\operatorname{Spec}(K[X]) = \{(0)\} \cup \{(f) \mid f \in K[X] \setminus K \text{ irreducible, monic}\}$

Ex: $A = \mathbb{Z}[i\sqrt{5}] = \{a+bi\sqrt{5} \mid a,b \in \mathbb{Z}\}$ is not a UFD:

$21 = 3\cdot 7 = 4^2+5\cdot 1^2 = (4+i\sqrt{5})(4-i\sqrt{5})$

$\forall \alpha \in A \quad N(\alpha) = \alpha\bar{\alpha} \neq 3, 7 \Rightarrow 3, 7, 4\pm i\sqrt{5} \in A$ are irreducible;

however, $A/3A$ is not a domain ($3 \mid 21$, $3 \nmid 4\pm i\sqrt{5}$).

Computing $A/3A$: write everything in terms of polynomials

("Kronecker's programme")

$ev_{i\sqrt{5}} : \mathbb{Q}[X] \longrightarrow \mathbb{Q}(i\sqrt{5}) = K = \mathrm{Frac}(A)$ induces

$g(X) \longmapsto g(i\sqrt{5})$

isomorphisms $\overline{ev_{i\sqrt{5}}} : \mathbb{Q}[X]/(X^2+5) \xrightarrow{\sim} K$

(X^2+5: minimal polynomial of $i\sqrt{5}$ over $\mathbb{Q}$)

$\mathbb{Z}[X]/\underbrace{((X^2+5)\mathbb{Q}[X] \cap \mathbb{Z}[X])}_{(X^2+5)\mathbb{Z}[X]} = \mathbb{Z}[X]/(X^2+5) \xrightarrow{\sim} \mathbb{Z}[i\sqrt{5}] = A$

$\overline{g(X)} \longmapsto g(i\sqrt{5})$

$g(X)$

$\mathbb{Z}[X]$

$\mathbb{F}_3[X] = \mathbb{Z}[X]/(3)$ $\qquad$ $\overline{g(X)}$

$\mathbb{Z}[X]/(X^2+5) = A \ni g(i\sqrt{5})$

$\mathbb{F}_3[X]/(X^2+5) = \mathbb{Z}[X]/(3, X^2+5) = A/3A \ni a+bi\sqrt{5} \pmod{3A}$

$\mathbb{F}_3[X]/(X^2-1)$ $\qquad$ $g(X) = a+bX$

$\mathbb{F}_3[X]/((X-1)(X+1)) = \mathbb{F}_3[X]/(X-1) \times \mathbb{F}_3[X]/(X+1)$

$\overline{ev_1}$ $\qquad$ $\overline{ev_{-1}}$

$\mathbb{F}_3 \times \mathbb{F}_3 \ni (a+b \pmod 3, a-b \pmod 3)$

$\longrightarrow (g(1) \pmod 3, g(-1) \pmod 3)$

Two projections: $A/3A \xrightarrow{\sim} \mathbb{F}_3 \times \mathbb{F}_3$

pr_1 $\qquad$ pr_2

$\mathbb{F}_3$ $\qquad$ $\mathbb{F}_3$

pr_1: $(a+b \pmod 3)$ $\qquad$ pr_2: $(a-b \pmod 3)$

$(3) \subset P_i = \mathrm{Ker}(A \longrightarrow A/3A \xrightarrow{pr_i} \mathbb{F}_3) \subset A$ ideal, $A/P_i = \mathbb{F}_3$

$P_i \in \mathrm{Spec}(A)$, $P_1 = \{a+bi\sqrt{5} \mid a,b \in \mathbb{Z},\ a+b \equiv 0 \pmod 3\} = (3, i\sqrt{5}-1)$

$P_2 = \{$ ——— " ——— , $a-b \equiv 0 \pmod 3\} = (3, i\sqrt{5}+1)$

Product:

$P_1P_2 = (9, 3i\sqrt{5}+3, 3i\sqrt{5}-3, -6) = (3, 3i\sqrt{5}) = 3A = (3)$

Similarly: $x^2+5 \equiv (x+3)(x+3) \pmod{7\mathbb{Z}[X]}$

$A/(7) = \mathbb{Z}[X]/(x^2+5, 7) = \mathbb{F}_7[X]/((x+3)(x+3)) \xrightarrow{\sim} \mathbb{F}_7 \times \mathbb{F}_7$

$\overline{g(X)} \longmapsto (g(3) \pmod 7, g(+3) \pmod 7)$

$Q_i = \ker(A \to A/7A \xrightarrow{pr_i} \mathbb{F}_7) \in \mathrm{Spec}(A)$, $A/Q_i = \mathbb{F}_7$

$Q_1 = (7, i\sqrt{5}+3)$, $Q_2 = (7, i\sqrt{5}-3)$

$P_1Q_1 = (3, i\sqrt{5}-1)(7, i\sqrt{5}+3) = (21, 3i\sqrt{5}+9, 7i\sqrt{5}-7, 2i\sqrt{5}-8) =$

$= (21, 3i\sqrt{5}+9, 2i\sqrt{5}-8)$ ($3i\sqrt{5}+9 = 2C$, $7i\sqrt{5}-7 = 2C + 2i\sqrt{5}-8$)

$= (21, i\sqrt{5}+17, 2i\sqrt{5}-8) = (21, i\sqrt{5}+17) = (21, i\sqrt{5}-4) = (i\sqrt{5}-4)$

($i\sqrt{5}+17 = 2C - 2\cdot 21$; $(-i\sqrt{5}-4)(i\sqrt{5}-4) = (4-i\sqrt{5})$)

$P_2Q_2 = (4+i\sqrt{5})$.

Summary: the non-unique factorisation in $\mathbb{Z}[i\sqrt{5}]$

$21 = 3\cdot 7 = (4+i\sqrt{5})(4-i\sqrt{5})$ ($3, 7, 4 \pm i\sqrt{5}$ irreducible)

can be refined into

$(3) = P_1P_2$, $(7) = Q_1Q_2$, $(4-i\sqrt{5}) = P_1Q_1$, $(4+i\sqrt{5}) = P_2Q_2$

$(21) = P_1P_2Q_1Q_2$.

The above example is a special case of the Kummer – Dedekind Theorem about decomposition (factorisation) of prime numbers into products of prime ideals in $\mathcal{O}_L$.

Prop. A = ring, $I, J \subset A$ ideals, $P \in \mathrm{Spec}(A)$.

If $P \supset IJ \Rightarrow P \supset I$ or $P \supset J$

(morally, "$P \mid IJ \Rightarrow P \mid I$ or $P \mid J$"; this is literally true if A = Dedekind ring)

Pf. If $P \not\supset I$ $\exists\, a \in I$, $a \notin P$.

$\forall b \in J$ $\quad ab \in IJ \subset P$, $a \notin P$ $\Rightarrow b \in P$ ($P \in \mathrm{Spec}(A)$); therefore $J \subset P$.

Prime ideals in geometry

K = field

$K[X_1, \dots, X_n]$ = regular functions (in the world of algebraic geometry) on the affine space $\mathbb{A}^n_K$ of dim $= n$ over K

Any ideal $I \subset K[X_1, \dots, X_n]$ defines an algebraic set $Z \subset \mathbb{A}^n_K$ given by the equations $\forall f \in I \quad f = 0$.

The quotient ring $K[X_1, \dots, X_n]/I = \mathcal{O}(Z)$ = the ring of regular functions on Z

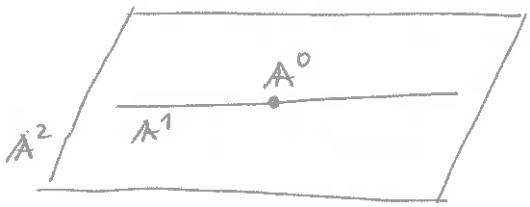
I is a prime ideal of $K[X_1, \dots, X_n] \iff Z \subset \mathbb{A}^n_K$ is irreducible

Ex: prime ideals

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subset \dots \subsetneq (X_1, \dots, X_n)$$

correspond to

$$\mathbb{A}^n_K \supset \underbrace{\begin{pmatrix}\text{hyperplane}\\ X_1 = 0\end{pmatrix}}_{\mathbb{A}^{n-1}_K} \supset \underbrace{\begin{pmatrix}\text{subspace}\\ X_1 = X_2 = 0\end{pmatrix}}_{\mathbb{A}^{n-2}_K} \supset \dots \supset \underbrace{\begin{pmatrix}\text{point}\\ X_1 = \dots = X_n = 0\end{pmatrix}}_{\mathbb{A}^0_K}$$



Def. The Krull dimension of a ring A is

$$\dim(A) = \sup\{r \geq 0 \mid \exists\, P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r,\ P_i \in \operatorname{Spec}(A)\} \in \{0, 1, 2, \dots\} \cup \{+\infty\}$$

Ex: K field $\Rightarrow$ $\dim K[X_1, \dots, X_n] = n$ (easy if $n \leq 2$)

Maximal ideals: **Def.** An ideal I of A is maximal if $I \neq A$ and if $I \subset J \neq A$ is an ideal $\Rightarrow J = I$.

Notation: $\operatorname{Max}(A) = \{m \subset A \mid \text{maximal ideal}\}$.

Prop. $I \in \operatorname{Max}(A) \iff A/I$ is a field.

Pr: $\forall x \notin I \quad (x) + I = A \iff A/I \neq 0 \iff A/I \neq 0$

$I \neq A \qquad \forall \bar{x} \in A/I \quad (\bar{x}) = A/I \iff A/I - \{0\} = (A/I)^*$

Cor. $\operatorname{Max}(A) \subset \operatorname{Spec}(A)$.

Ex: $A = PID \Rightarrow \mathrm{Spec}(A) = \{(0)\} \cup \underbrace{\{(x) \mid x \in A \text{ irreducible}\}}_{\mathrm{Max}(A)}$

Rmks: (1) One can show, using Zorn's lemma, that for an ideal $I \subsetneq A$ in any ring A there exists $m \in \mathrm{Max}(A)$, $m \supset I$. This will be automatic for all the rings we are interested in, such as $\mathcal{O}_L$ ($[L:\mathbb{Q}] < \infty$), since they have very strong finiteness properties.

---

(2) Any domain A satisfies:

$\dim(A) = 0 \iff \mathrm{Spec}(A) = \{(0)\} \Rightarrow \mathrm{Max}(A) = \{(0)\} \iff A = \text{field}$.

$\Downarrow$

$\mathrm{Spec}(A) = \{(0)\}$.

---

(3) Any domain A satisfies:

$\dim(A) = 1 \iff A \neq \text{field}$ and $\mathrm{Spec}(A) = \{(0)\} \cup \underbrace{\mathrm{Max}(A)}_{\neq \emptyset}$.

Def. A ring A is noetherian (after Emmy Noether) if every ideal $I \subset A$ is finitely generated ($I = (\alpha_1, \dots, \alpha_n)$)

[Ex: $A = PID$] $\Updownarrow$

if $I_1 \subset I_2 \subset \dots \subset A$ are ideals, then $\exists j \ \forall k \geq j \ \ I_k = I_j$

Pf: $\Downarrow$ $I = \bigcup_{j \geq 1} I_j$ ideal $\Rightarrow I = (\alpha_1, \dots, \alpha_n)$, $\exists j$ $\alpha_1, \dots, \alpha_n \in I_j$

$\Rightarrow I = I_j$.

$\Uparrow$ If $I \subset A$ is not finitely generated, then $\forall \alpha_1 \in I$

$I_1 = (\alpha_1) \subsetneq I$, $\forall \alpha_2 \in I \setminus I_1$ $I_1 \subsetneq I_2 = (\alpha_1, \alpha_2) \subsetneq I$ etc.

Ex: If $A \supset \mathbb{Z}$, $(A,+) \simeq \mathbb{Z}^n$ (more generally, if $(A,+)$ is a finitely generated abelian group, then $(I,+)$ ——— " ———, for every ideal $I \subset A \Rightarrow A$ is noetherian.

Two statements from long time ago (left unproved)

Prop. $\forall n \geq 1 \quad \mathbb{Z}[\xi_n] \cap \mathbb{Q} = \mathbb{Z}$ $\qquad (\xi_n = e^{2\pi i/n})$

Pf. ξ_n is a root of $X^n - 1 \Rightarrow \xi_n \in \mathcal{O}_L$, $L = \mathbb{Q}(\xi_n)$

$\Rightarrow \mathbb{Z}[\xi_n] \subset \mathcal{O}_L$, $\mathbb{Z}[\xi_n] \cap \mathbb{Q} \subset \mathcal{O}_L \cap \mathbb{Q} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Prop. $A = \text{PID} \Rightarrow A$ UFD

Pf. We know that $A = \text{PID} \Rightarrow$ Euclid's Lemma holds in A

$\Rightarrow$ uniqueness of factorisation. We must show the existence of factorisation: $\forall a \in A \setminus \{0\}$ $\exists r \geq 0$ $\exists u \in A^*$ $\exists x_1, \dots, x_r \in A$ irreducible $a = u x_1 \cdots x_r$.

If $a \neq u x_1 \cdots x_r$, then $\exists a_1, b_1 \in A$ $(a_1, b_1 \notin A^* \cup \{0\})$ $a = a_1 b_1$ (since $a \notin A^* \cup \{0\}$ and $a \neq$ irreducible) $\Rightarrow (a) \subsetneq (a_1), (b_1)$.

At least one of a_1, b_1 (say, a_1) cannot be written as $u x_1 \cdots u_r \Rightarrow a_1 = a_2 b_2$, $a_2, b_2 \notin A^* \cup \{0\}$, etc.

$\Rightarrow (a) \subsetneq (a_1) \subsetneq (a_2) \subset \cdots$ – impossible, since A is a noetherian ring.

Dedekind rings

Def A **Dedekind ring** is an integral domain A whose all fractional ideals are invertible, $I(A) = I_{inv}(A)$ ($\Leftrightarrow$ fractional ideals of A form an (abelian) group under multiplication).

the **ideal class group** of A is $Cl(A) = I(A)/P(A)$ (principal fractional ideals)

($Cl(A) = Pic(A)$ in this case).

Ex: (1) $A = K$ field, $Cl(A) = 0$.

(2) $A = PID$, $Cl(A) = 0$.

(3) $A = \mathcal{O}_K$ ($[K:\mathbb{Q}] < \infty$) the ring of integers in a number field K; we know that $|Cl(\mathcal{O}_K)| < \infty$.

Classical notation: $Cl_K = Cl(\mathcal{O}_K)$, $h_K = |Cl(\mathcal{O}_K)|$ the class number of K

Thm of Lagrange $\Rightarrow$ $\forall I \in Cl_K$ $I^{h_K} = (\alpha)$ is principal.

Properties of Dedekind rings

(A = Dedekind ring, $K = Frac(A)$)

(1) $I_1, I_2, J \in I(A)$, $I_1 J = I_2 J \Rightarrow I_1 \underbrace{JJ^{-1}}_{A} = I_2 \underbrace{JJ^{-1}}_{A} \Rightarrow I_1 = I_2$.

(2) A is a **noetherian ring** (later: every ideal is generated by at most 2 elements)

Pf: $\forall I \in I(A)$ $II^{-1} = (1) = A \Rightarrow 1 = \sum_{i=1}^{n} \alpha_i \beta_i$, $\alpha_i \in I$, $\beta_i \in I^{-1}$

$\forall x \in I$ $x = \sum_{i=1}^{n} \alpha_i \underbrace{(x\beta_i)}_{\in A} \in (\alpha_1, \dots, \alpha_n) = A\alpha_1 + \dots + A\alpha_n \subset I \Rightarrow I = (\alpha_1, \dots, \alpha_n)$.

---

(3) **Def**. For $(0) \neq I, J \subset A$ ideals, we say that **I divides J** ($I|J$) if $\exists$ ideal $I_1 \subset A$ such that $II_1 = J$.

Prop. $I|J \Leftrightarrow I \supset J$. **Cor**: $\forall P \in Spec(A) \setminus \{(0)\}$ $P|IJ \Rightarrow P|I$ or $P|J$

Pf ($\Rightarrow$) $II_1 = J \Rightarrow J = II_1 \subset IA = I$.

($\Leftarrow$) $I \supset J \Rightarrow A = II^{-1} \supset JI^{-1} = I_1$, $I_1 I = JI^{-1}I = JA = J$.

---

(4) $\forall I_1 \subsetneq A$ ideal $\exists$ $m \in Max(A)$ $m \supset I_1$:

if $I_1 \neq$ maximal $\exists$ $I_1 \subsetneq I_2 \subsetneq A$ ideal

if $I_2 \neq$ — " — $\subsetneq I_3 \subsetneq A$ ideal etc.

A = noetherian $\Rightarrow$ $\exists n$ I_n = maximal.

(5) $\forall\ (0)\neq I\subset A$ ideal $\exists r\geq 0$ $\exists m_i\in \mathrm{Max}(A)$ $I=m_1\cdots m_r$.

Pf. If $I=A\Rightarrow r=0$. If $I\neq A$ $\exists\, m_1\in\mathrm{Max}(A)$ $m_1\supset I$ $\overset{(3)}{\Rightarrow}$ $m_1\mid I$, $I=m_1I_1$
$I=m_1I_1 \overset{(1)}{\subsetneq} I_1=AI_1$. Repeat with I_1; if $I_1\neq A$ get $I_1=m_2I_2\subsetneq I_2$.
this must stop by (2) $\Rightarrow$ get $I=m_1\cdots m_rI_r$, $I_r=A$.

(6) $\mathrm{Spec}(A)=\{(0)\}\cup\mathrm{Max}(A)$ ($\Leftrightarrow \dim(A)\leq 1$; of course, $\dim(A)=0 \Leftrightarrow A=$ field)

Pf: If $(0)\neq P\in\mathrm{Spec}(A)\overset{(5)}{\Rightarrow} P=m_1\cdots m_r$, $r\geq 1$, $m_i\in\mathrm{Max}(A)$
(3) Cor $\Rightarrow \exists i$ $P\supset m_i\Rightarrow P=m_i$, by maximality.

(7) If $(0)\neq I\subset A$ ideal, $I=m_1\cdots m_r=m_1'\cdots m_s'$, $m_i,m_j'\in\mathrm{Max}(A)$
$\Rightarrow r=s$, $m_i=m_i'$ (after renumbering the m_j's).

Pf: If $r=0\Rightarrow I=A\Rightarrow s=0$. If $r\geq 1$: $m_1\supset I=m_1'\cdots m_s'\Rightarrow \exists i$ $m_1\supset m_i'$
After renumbering, $m_1\supset m_1'\Rightarrow m_1=m_1'\Rightarrow m_2\cdots m_r=m_1^{-1}I=m_1'^{-1}I=m_2'\cdots m_s'$ etc.

(8) Cor. of (5)–(7): non-zero ideals $I\subset A$ have unique factorisation

$$\boxed{I=\prod_P P^{v_P(I)}}$$

, $P\in\mathrm{Spec}(A)\setminus\{(0)\}$ $(=\mathrm{Max}(A))$, $v_P(I)\in\mathbb{N}=\mathbb{Z}_{\geq 0}$
(all but finitely many $v_P(I)$ are $=0$).

$\Rightarrow$
- $I=J\Leftrightarrow \forall P$ $v_P(I)=v_P(J)$
- $v_P(IJ)=v_P(I)+v_P(J)$
- $I\mid J\Leftrightarrow \forall P$ $v_P(I)\leq v_P(J)$

($(0)\neq I,J\subset A$ ideals)

- $I+J$ satisfies $I+J\supset IJ$; if $I_1\supset IJ\Rightarrow I_1\supset I+J$
$(I+J)\mid IJ$ $\quad$ $I_1\mid IJ$ $\quad$ $I_1\mid(I+J)$
$\Rightarrow I+J=\gcd(I,J):=\prod_P P^{\min(v_P(I),v_P(J))}$
- $IJ\mid \mathrm{lcm}(I,J):=\prod_P P^{\max(v_P(I),v_P(J))}$ and if
$IJ\mid I_2\Rightarrow \mathrm{lcm}(I,J)\mid I_2$. Therefore $\mathrm{lcm}(I,J)=I\cap J$.

(9) Extension of (8) to fractional ideals:
for $I\in\mathcal{I}(A)$, $n\in\mathbb{Z}_{>0}$ let $I^{-n}=(I^{-1})^n$ $(I^0=(1)=A)$.
Then: $\forall\, I\in\mathcal{I}(A)$ $\exists$ $(0)\neq I_1,I_2\subset A$ ideals
$I=I_1I_2^{-1}$ (even with $I_2=(\beta)$ principal), $I_j=\prod_P P^{v_P(I_j)}$
$\Rightarrow I=\prod_P P^{v_P(I)}$ $\quad$ $v_P(I)=v_P(I_1)-v_P(I_2)\in\mathbb{Z}$
depends only on I, not on I_1,I_2
$v_P(IJ)=v_P(I)+v_P(J)$ $\quad$ (all but finitely many v_P are $=0$)

(10) For $I \in \mathcal{I}(A)$, $\left[I \subset A \iff \forall P \quad v_P(I) \geq 0 \right]$

Pf: ($\Leftarrow$) if all $v_P(I) \geq 0 \Rightarrow I = \prod_P P^{v_P(I)} \subset \prod_P A = A$. ($\Rightarrow$) (8) + uniqueness of $v_P(I)$

(11) Algebraic reformulation: ideals $\longleftrightarrow$ divisors

Def. A divisor of A is a formal finite sum $D = \sum_P n_P P$, $P \in \mathrm{Spec}(A) \setminus \{(0)\}$ $(= \mathrm{Max}(A))$, $n_P \in \mathbb{Z}$, all but finitely many n_P are $= 0$.

$\mathrm{Div}(A) = \{$ divisors of $A\}$ $\left(= \bigoplus_P \mathbb{Z} \cdot P\right)$ is an abelian group under

$$\left(\sum n_P P\right) + \left(\sum n'_P P\right) = \sum (n_P + n'_P) P.$$

Prop. The maps

$$\begin{array}{ccc} \mathcal{I}(A) & \longrightarrow & \mathrm{Div}(A) \\ \downarrow & & \downarrow \\ I & \longmapsto & \sum v_P(I) P \end{array} \quad , \quad \begin{array}{ccc} \mathrm{Div}(A) & \longrightarrow & \mathcal{I}(A) \\ \downarrow & & \downarrow \\ \sum n_P P & \longmapsto & \prod P^{n_P} \end{array}$$

are mutually inverse group morphisms $\Rightarrow$ group isomorphisms.

Pf: Follows from $v_P(IJ) = v_P(I) + v_P(J)$ and $v_{P_1}(P_2) = \begin{cases} 1 & P_1 = P_2 \\ 0 & P_1 \neq P_2 \end{cases}$.

(12) Discrete valuations of $K = \mathrm{Frac}(A)$ attached to $\{P\}$:

For each $P \in \mathrm{Spec}(A) \setminus \{(0)\} = \mathrm{Max}(A)$ we obtain

$$\begin{array}{rccl} v_P : & K & \longrightarrow & \mathbb{Z} \cup \{+\infty\} \\ & \alpha & \longmapsto & \begin{cases} +\infty & \text{if } \alpha = 0 \\ v_P(\alpha) & \text{if } \alpha \neq 0 \end{cases} \end{array}$$

(so that $\forall \alpha \in K^* \quad (\alpha) = \prod_P P^{v_P(\alpha)}$). Properties:

- $v_P(xy) = v_P(x) + v_P(y)$
- $v_P(x+y) \geq \min(v_P(x), v_P(y))$
- $v_P(K^*) = \mathbb{Z}$ $\left(\forall n \geq 0 \quad P^n \supsetneq P^{n+1} = P \cdot P^n \neq (0) \right) \Rightarrow \exists \alpha \in P^n - P^{n+1}$ $v_P(\alpha) = n = -v_P(\alpha^{-1})$
- $\alpha \in A \overset{(10)}{\iff} \forall P \quad v_P(\alpha) \geq 0$.

(13) A is integrally closed.

Pf: If $\alpha = \frac{a}{b} \in K$, $\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0$ $(a, b, a_i \in A) \Rightarrow$

$a^n + \underbrace{a_1 a^{n-1} b + \cdots + a_{n-1} a b^{n-1} + a_n b^n}_{} = 0$. If $\alpha \notin A \Rightarrow \exists P \; v_P(\alpha) < 0$

$\Rightarrow v_P(a) < v_P(b) \Rightarrow v_P(-\text{---}) \geq (n-1) v_P(a) + v_P(b) > n v_P(a) = v_P(a^n)$

contradiction.

(14) A (Dedekind ring) $=$ UFD $\iff$ $A=$ PID $(\iff Cl(A)=0)$

Pf: $\Leftarrow$ known

$\Rightarrow$ $x\in A$ irreducible $\overset{A\text{ UFD}}{\Longrightarrow}$ $(x)\in \mathrm{Spec}(A)\setminus\{(0)\}=\mathrm{Max}(A)$

$\forall P\in \mathrm{Spec}(A)\setminus\{(0)\}$ $\exists\, 0\neq a\in P$, $a=u x_1\cdots x_r$, $u\in A^*$, x_i irreducible, $r\geq 1$

$\Rightarrow$ $P\supset (a)=(x_1)\cdots(x_r)\Rightarrow \exists i$ $P\supset(x_i)\Rightarrow P=(x_i)$ principal ($(x_i)\in\mathrm{Max}(A)$)

$0\neq I\subset A$ ideal $\Rightarrow I=\prod \underbrace{P^{v_P(I)}}_{\text{principal}}\Rightarrow I$ principal.

Rmk: One can show that PID's are precisely UFD's of $\dim\leq 1$.

(15) The Chinese Remainder Theorem:

(a) $\gcd(I,J)=(1)\Rightarrow I+J=(1)\Rightarrow A/IJ\xrightarrow{\sim} A/I\times A/J$

$\Downarrow$ (induction on r) $\quad IJ=I\cap J$

(b) $P_1,\dots,P_r\in\mathrm{Spec}(A)\setminus\{(0)\}$ distinct $\Rightarrow A/P_1^{n_1}\cdots P_r^{n_r}\xrightarrow{\sim} A/P_1^{n_1}\times\cdots\times A/P_r^{n_r}$

$n_1,\dots,n_r\in\mathbb{Z}_{>0}$ $\qquad\qquad\Downarrow$

(c) ——— $\Rightarrow$ $\exists\, a\in A$ $\forall i=1,\dots,r$ $\underbrace{a\equiv a_i \pmod{P_i^{n_i}}}_{v_{P_i}(a-a_i)\geq n_i}$

$a_1,\dots,a_r\in A$

(16) Prop. $P\in\mathrm{Spec}(A)\setminus\{(0)\}$, $n\geq 1$, $a\in A$. Then:

$a\pmod{P^n}\in(A/P^n)^*\Longleftarrow v_P(a)=0\iff a\pmod P\in(A/P)^*\Longleftarrow P\nmid(a)$.

Pf: $\Downarrow$

$1\in(a)+P^n\iff \gcd((a),P^n)=(1)\iff v_P(a)=0$.

(17) Approximation: let $P_1,\dots,P_r\in\mathrm{Spec}(A)\setminus\{0\}$ distinct, $m_1,\dots,m_r\in\mathbb{Z}_{\geq 0}$

Prop: (a) $\exists\, a\in A$ $\forall i=1,\dots,r$ $v_{P_i}(a)=m_i$ $(\iff a\in P_i^{m_i}-P_i^{m_i+1})$.

(b) $\forall\, a_1,\dots,a_r\in K=\mathrm{Frac}(A)$ $\exists\, x\in K$ $\forall i=1,\dots,r$ $v_{P_i}(x-a_i)\geq m_i$.

Pf: (a) Apply (15c) to $n_i=1+m_i$, $a_i\in P_i^{m_i}\setminus P_i^{m_i+1}$.

(b) By (a), $\exists\, b\in A$ $\forall i$ $v_{P_i}(b)=1$. For $N\gg 0$, $\forall i$ $b^N a_i\in A$.

Apply (15c) to $b^N a_i$, $n_i=N+m_i\Rightarrow$ get $a\in A$, $v_{P_i}(a-b^N a_i)\geq n_i$ for all $i\Rightarrow$ take $x=b^{-N}a$.

(18) Prop. $(0) \neq I \subset A$ ideal, $0 \neq a \in I \Rightarrow \exists\, b \in I$ $(a,b) = I$

Pf. $(a) \subset I$, $I = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} \mid (a) = \mathfrak{p}_1^{m_1'} \cdots \mathfrak{p}_r^{m_r'} Q_1^{n_1} \cdots Q_s^{n_s}$, $\forall i = 1, \dots, r$ $m_i' \geq m_i$

By (17a), $\exists\, b \in A$ $\forall i = 1, \dots, r$ $v_{\mathfrak{p}_i}(b) = m_i$ ($\Rightarrow I \mid (b) \Rightarrow b \in I$)

$\forall j = 1, \dots, s$ $v_{Q_j}(b) = 0$

$\Rightarrow (a,b) = \gcd((a),(b)) = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} = I$.

---

(19) Prop. $\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{0\}$, $a \in A$, $r = v_{\mathfrak{p}}(a) \geq 1 \Rightarrow$ multiplication by a defines a morphism of $A/\mathfrak{p}$-vector spaces $f: A/\mathfrak{p} \longrightarrow \mathfrak{p}^r/\mathfrak{p}^{r+1}$, $x \pmod{\mathfrak{p}} \longmapsto ax \pmod{\mathfrak{p}^{r+1}}$, which is an isomorphism.

Pf: If $x \in A$, then $f(x \pmod{\mathfrak{p}}) = 0 \Leftrightarrow ax \in \mathfrak{p}^{r+1} \Leftrightarrow \underbrace{v_{\mathfrak{p}}(ax)}_{r + v_{\mathfrak{p}}(x)} \geq r+1 \Leftrightarrow x \in \mathfrak{p}$.

Therefore $\ker(f) = 0$, f is injective.

$\underbrace{(a)}_{aA} + \mathfrak{p}^{r+1} = \gcd((a), \mathfrak{p}^{r+1}) = \mathfrak{p}^{\min(v_{\mathfrak{p}}(a), r+1)} = \mathfrak{p}^r \Rightarrow \forall\, b \in \mathfrak{p}^r \ \exists\, x \in A$

$ax \equiv b \pmod{\mathfrak{p}^{r+1}}$

$\Rightarrow$ f is surjective.

Exercise. Let A = Dedekind ring, $K = \mathrm{Frac}(A)$, $\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{(0)\}$.

(a) $A_{\mathfrak{p}} = \{a \in K \mid v_{\mathfrak{p}}(a) \geq 0\}$ is a subring of K containing A.

(b) $m_{\mathfrak{p}} = \{a \in K \mid v_{\mathfrak{p}}(a) > 0\}$ is an ideal of $A_{\mathfrak{p}}$.

(c) The canonical map $\underbrace{A/\mathfrak{p}}_{\text{field}} \longrightarrow A_{\mathfrak{p}}/m_{\mathfrak{p}}$ is an isomorphism of rings.

(d) $A_{\mathfrak{p}}^* = \{a \in K \mid v_{\mathfrak{p}}(a) = 0\}$

(e) $I(A_{\mathfrak{p}}) = \{\pi^n A_{\mathfrak{p}} \mid n \in \mathbb{Z}\}$ (for any $\pi \in K$, $v_{\mathfrak{p}}(\pi) = 1$)

[$A_{\mathfrak{p}}$ (a generalisation of $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$) is the valuation ring of the discrete valuation $v_{\mathfrak{p}}$ on K.]

Question: If B = domain, $\dim(B) = 1$, $B \neq$ Dedekind, is there unique factorisation for invertible ideals?

NO! Ex: $B = \mathbb{Z}[i\sqrt{11}]$, $I = (4, 1+i\sqrt{11})$, $I^2 = (2)(4, 1-i\sqrt{11})$,

$I^3 = (2)(4) = (2)^3$ $\exists!\ m \in \mathrm{Max}(B)$ $m \supset I$

$m = (2, 1+i\sqrt{11})$, $m \neq$ invertible

$E_{\mathbb{Q}(i\sqrt{11})}(m) = \mathbb{Z}\left[\frac{1+i\sqrt{11}}{2}\right] \supsetneq B$

Abstract characterisation of Dedekind rings

Fans of abstract algebra may appreciate the fact that Dedekind rings are characterised by the properties (2), (6) and (13). We are not going to use this statement, though. For the sake of completeness, we include the proof.

Thm. An integral domain A is a Dedekind ring $\Leftrightarrow$ (1) A is noetherian; (2) every non-zero prime ideal of A is maximal ($\Leftrightarrow \dim(A) \le 1$); (3) A is integrally closed.

Pf. **Lemma 1.** If A satisfies (1), then every ideal $(0) \neq I \subset A$ contains a product $P_1 \cdots P_r$, for some $P_i \in \mathrm{Spec}(A) \setminus \{0\}$ (not necessarily distinct). [Moralf, "$I \mid P_1 \cdots P_r$"].

Pf. Assume $S = \{I \subset A \mid I \neq (0) \text{ ideal not containing any } P_1 \cdots P_r\} \neq \emptyset$. Then S has a maximal element I (otherwise it would contain $I_1 \subsetneq I_2 \subsetneq I_3 \cdots$, in contradiction to (1)). Clearly, $I \neq A$, $I \notin \mathrm{Spec}(A) \Rightarrow \exists a, b \in A$, $a, b \notin I$, $ab \in I$. The ideals $I + (a) \supsetneq I$, $I + (b) \supsetneq I$ cannot lie in $S \Rightarrow I + (a) \supset P_1 \cdots P_r$, $I + (b) \supset P_1' \cdots P_s'$ ($P_i, P_j' \in \mathrm{Spec}(A) \setminus \{0\}$) $\Rightarrow I = (I + (a))(I + (b)) \supset P_1 \cdots P_r P_1' \cdots P_s'$ contradiction.

Lemma 2. If A satisfies (1), (2) and if $(0) \neq I \subsetneq A$ is an ideal, then $I^{-1} \supsetneq A$.

Pf. Choose $a \in I \setminus \{0\} \xRightarrow{\text{Lemma 1}} (a) \supset P_1 \cdots P_r$, $P_i \in \mathrm{Spec}(A) \setminus \{0\}$. Can assume r is minimal ($I \neq A \Rightarrow r \ge 1$).
$\exists P \in \mathrm{Max}(A)$ $P \supset I \supset (a) \supset P_1 \cdots P_r \Rightarrow \exists i$ (say, $i = 1$) $P \supset P_i = P_1$.
$\dim(A) \le 1 \Rightarrow P = P_1$. Minimality of $r \Rightarrow \exists b \in P_2 \cdots P_r$, $b \notin (a)$.
Then $b/a \in K = \mathrm{Frac}(A)$, $b/a \notin A$, $(b/a) I \subset \frac{P_2 \cdots P_r I}{a} \subset \frac{P_1 \cdots P_r}{a} \subset A$
$\Rightarrow b/a \in I^{-1} \setminus A$.

Lemma 3. If A satisfies (1), (2), (3), then $\forall I \in \mathcal{I}(A)$ $I I^{-1} = A$.

Pf. $J = I I^{-1} \subset A$ is a non-zero ideal of A. Let $\alpha \in J^{-1}$; then $\alpha I I^{-1} \subset A$. $\forall \beta \in I^{-1}$ $\alpha \beta I \subset A \Rightarrow \alpha\beta \in I^{-1}$, hence $\alpha \in E_K(I^{-1}) \Rightarrow \alpha \in K$ is integral over $A \xRightarrow{(3)} \alpha \in A$.
(I^{-1} is an A-module of finite type.)
Therefore $J^{-1} \subset A \xRightarrow{\text{Lemma 2}} J = A$.

Back to number fields

Let $\underbrace{[K:\mathbb{Q}]}_{n} < \infty$; then $\mathcal{O}_K$ is a Dedekind ring and $(\mathcal{O}_K, +) \simeq \mathbb{Z}^n$.

Prop.–Def. If $(0) \neq I \subset \mathcal{O}_K$ is an ideal, then its **norm** is $N(I) = |\mathcal{O}_K / I| = (\mathcal{O}_K : I)$.

(1) $N(I) < \infty$.

(2) If $I = (\alpha)$, $\alpha \in \mathcal{O}_K \setminus \{0\}$, then $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

(3) If $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \setminus \{(0)\}$, then $\underbrace{\mathcal{O}_K/\mathfrak{p}}_{k(\mathfrak{p})}$ is a finite field, $k(\mathfrak{p}) \supset \mathbb{F}_p$, $\mathfrak{p} \mid (p)$ and $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$, where $f_{\mathfrak{p}} = [k(\mathfrak{p}) : \mathbb{F}_p]$.

(4) If $\gcd(I, J) = (1) \Rightarrow N(IJ) = N(I)\,N(J)$.

(5) $N(IJ) = N(I)\,N(J)$

(6) $N\left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}\right) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{n_{\mathfrak{p}}}$.

Pf. (1) $(\mathcal{O}_K, +) = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i$; $\exists\, 0 \neq \beta \in I \Rightarrow \bigoplus_{i=1}^{n} \mathbb{Z}\beta\alpha_i \subset I \subset \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i \Rightarrow I \simeq \mathbb{Z}^n$; $\underbrace{\bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i}_{\mathcal{O}_K}$ $(\mathcal{O}_K : I) < \infty$.

(2) $\alpha(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n) M(\alpha)$, $M(\alpha) \in M_n(\mathbb{Z})$

$\Rightarrow (\mathcal{O}_K : \alpha\mathcal{O}_K) = |\det(M(\alpha))|$, but $\det(M(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$.

(3) $|k(\mathfrak{p})| < \infty$ & (1) $\Rightarrow \exists!$ prime number p such that $k(\mathfrak{p}) \supset \mathbb{F}_p$ ($\Leftrightarrow p\mathcal{O}_K \subset \mathfrak{p} \Leftrightarrow \mathfrak{p} \mid (p)$), $|k(\mathfrak{p})| = p^{[k(\mathfrak{p}) : \mathbb{F}_p]}$

(4) The Chinese Remainder Theorem: $\mathcal{O}_K / IJ \simeq \mathcal{O}_K/I \times \mathcal{O}_K/J$.

(5) Writing $I = \prod \mathfrak{p}^{r_{\mathfrak{p}}(I)}$ and $J = \prod \mathfrak{p}^{r_{\mathfrak{p}}(J)}$, (4) $\Rightarrow$ it is enough to show that $N(\mathfrak{p}^r) = N(\mathfrak{p})^r$ $(\forall r \geq 1)$. We have

$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \dots \supset \mathfrak{p}^r \Rightarrow N(\mathfrak{p}^r) = (\mathcal{O}_K : \mathfrak{p}^r) = \prod_{i=1}^{r} (\mathfrak{p}^{i-1} : \mathfrak{p}^i)$.

Fix $a_i \in \mathfrak{p}^{i-1} \setminus \mathfrak{p}^i$; we know that multiplication by a_i induces an isomorphism of $k(\mathfrak{p})$-vector spaces

$\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^{i-1}/\mathfrak{p}^i \Rightarrow (\mathfrak{p}^{i-1} : \mathfrak{p}^i) = (\mathcal{O}_K : \mathfrak{p}) = N(\mathfrak{p}) \Rightarrow N(\mathfrak{p}^r) = N(\mathfrak{p})^r$.

(6) Follows from (5).

Cor: The norm of any **fractional ideal** $N(IJ^{-1}) := N(I)\,N(J)^{-1} \in \mathbb{Q}_{>0}$ is well-defined.

Moreover, $N(I) = \underbrace{(\mathcal{O}_K : I)}_{\text{generalised index}}$, for any $I \in \mathcal{I}(\mathcal{O}_K)$.

Pf: $I = J(\beta)^{-1}$, $J \subset \mathcal{O}_K$, $\beta \in \mathcal{O}_K \setminus \{0\} \Rightarrow N(I) = \dfrac{N(J)}{|N_{K/\mathbb{Q}}(\beta)|} = (\mathcal{O}_K : I)$

as in the case $n = 2$.

Prop. (Minkowski's bound) Let $[K:\mathbb{Q}]=n$, $K_{\mathbb{R}}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$.

Every ideal class $C\in Cl_K=Cl(\mathcal{O}_K)$ contains an ideal $I\subset\mathcal{O}_K$ such that $N(I)\le \underbrace{\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}}_{\text{Minkowski's constant of } K}$.

Pf. Let $J\in C^{-1}$; we know that $\exists\ \beta\in J\setminus\{0\}$ such that ($J\in I(\mathcal{O}_K)$) $|N_{K/\mathbb{Q}}(\beta)|\le\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}(\mathcal{O}_K:J)$.

The ideal $I=(\beta)J^{-1}\subset JJ^{-1}=\mathcal{O}_K$ lies in $(C^{-1})^{-1}=C$ and satisfies $N(I)=|N_{K/\mathbb{Q}}(\beta)|/N(J)\le\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}\underbrace{\frac{(\mathcal{O}_K:J)}{N(J)}}_{=1}$

(for example, we could have taken $J\subset\mathcal{O}_K$)

Exercise. Let $[K:\mathbb{Q}]=n$, $\mathcal{O}_K=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$, $\sigma_1,\dots,\sigma_n:K\hookrightarrow\mathbb{C}$,

Write D_K as $\det(N)^2$, where $N_{ij}=\sigma_i(\alpha_j)$ $(1\le i,j\le n)$,

and show that $\det(N)=\underbrace{\sum_{\tau\in A_n}\prod_{j=1}^{n}\sigma_{\tau(j)}(\beta_j)}_{A}-\underbrace{\sum_{\tau\in S_n\setminus A_n}\prod_{j=1}^{n}\sigma_{\tau(j)}(\beta_j)}_{B}$,

where $A+B,\ AB\in\mathbb{Q}$.

Deduce that $A+B,\ AB\in\mathbb{Z}$ and $D_K=(A+B)^2-4AB\equiv 0,1\pmod 4$.

Exercise. Let $K,L\subset\mathbb{C}$ be subfields such that $KL\subset\mathbb{C}$ (the smallest subfield containing both K and L) satisfies $[KL:\mathbb{Q}]=\underbrace{[K:\mathbb{Q}]}_{m}\underbrace{[L:\mathbb{Q}]}_{n}<\infty$. Show that:

(1) $\forall\alpha\in K\ \forall\beta\in L$ $\mathrm{Tr}_{KL/K}(\alpha\beta)=\alpha\,\mathrm{Tr}_{L/\mathbb{Q}}(\beta)$, $\mathrm{Tr}_{KL/L}(\alpha\beta)=\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)\beta$.

(2) If $\left.\begin{aligned}\mathcal{O}_K&=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_m\\ \mathcal{O}_L&=\mathbb{Z}\beta_1\oplus\cdots\oplus\mathbb{Z}\beta_n\end{aligned}\right\}\Rightarrow KL=\mathbb{Q}\alpha_1\beta_1\oplus\cdots\oplus\mathbb{Q}\alpha_m\beta_n$

(3) If $\alpha=\sum_{i,j}a_{ij}\alpha_i\beta_j\in\mathcal{O}_{KL}$ $(a_{ij}\in\mathbb{Q})$, show, by considering $\mathrm{Tr}_{KL/L}(\alpha\alpha_{i'})$ (resp. $\mathrm{Tr}_{KL/K}(\alpha\beta_{j'})$) that $D_K a_{ij}\in\mathbb{Z}$ (resp. $D_L a_{ij}\in\mathbb{Z}$).

(4) Show that $\mathcal{O}_K\mathcal{O}_L\left(=\bigoplus_{i,j}\mathbb{Z}\alpha_i\beta_j\right)\subset\mathcal{O}_{KL}\subset\frac{1}{d}\mathcal{O}_K\mathcal{O}_L\left(=\bigoplus_{i,j}\mathbb{Z}\frac{\alpha_i\beta_j}{d}\right)$, where $d=\gcd(D_K,D_L)$. In particular, $\mathcal{O}_{KL}=\mathcal{O}_K\mathcal{O}_L$ if $d=1$.

Factorisation of primes

Recall: If $K=\mathbb{Q}(i)$, then $\mathcal{O}_K=\mathbb{Z}[i]$ and a prime number p factors in the PID $\mathbb{Z}[i]$ as follows:

- $p=2 \Rightarrow 2=(-i)(1+i)^2$, $\mathbb{Z}[i]/(2) \simeq \mathbb{F}_2[X]/(X^2)$, $i \leftrightarrow X+1$
- $p\equiv 3 \pmod 4 \Rightarrow p$ is irreducible in $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ and $i \leftrightarrow X$

$$\mathbb{Z}[i]/(p) = \mathbb{Z}[X]/(p, X^2+1) = \mathbb{F}_p[X]/(X^2+1) \simeq \mathbb{F}_{p^2}$$

$\left(\frac{-1}{p}\right) = -1 \Rightarrow$ irreducible in $\mathbb{F}_p[X]$

- $p\equiv 1 \pmod 4 \Rightarrow p=a^2+b^2=\underbrace{(a+bi)}_{\pi}\underbrace{(a-bi)}_{\bar{\pi}}$, $a\pm bi \in \mathbb{Z}[i]$ irreducible, $a\pm bi \not\sim a\mp bi$

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi}) = \mathbb{F}_p \times \mathbb{F}_p$$

General case: $K\supset\mathbb{Q}$, $[K:\mathbb{Q}]=n<\infty$

p prime number $\Rightarrow$ $(p)=p\mathcal{O}_K=\prod_{\mathfrak{P}\mid p}\mathfrak{P}^{e_{\mathfrak{P}}}$, $e_{\mathfrak{P}}:=v_{\mathfrak{P}}((p))$

$\mathfrak{P}\mid p \Leftrightarrow \underbrace{\mathcal{O}_K/\mathfrak{P}}_{k(\mathfrak{P})=\text{the residue field of }\mathfrak{P}} \supset \mathbb{F}_p$ $\qquad f_{\mathfrak{P}}:=[k(\mathfrak{P}):\mathbb{F}_p]$

Def: $e_{\mathfrak{P}}=v_{\mathfrak{P}}((p))$ = the ramification index of $\mathfrak{P}$ over p

$\mathfrak{P}$ is ramified in $K/\mathbb{Q}$ if $e_{\mathfrak{P}}>1$

p ——————"—————— if $\exists\,\mathfrak{P}\mid p$ $e_{\mathfrak{P}}>1$

Thm. $\sum_{\mathfrak{P}\mid p} e_{\mathfrak{P}} f_{\mathfrak{P}} = n = [K:\mathbb{Q}]$, $\qquad N(\mathfrak{P})=p^{f_{\mathfrak{P}}}$.

Pf: $\underbrace{N((p))}_{|N_{K/\mathbb{Q}}(p)|} = N\left(\prod_{\mathfrak{P}\mid p}\mathfrak{P}^{e_{\mathfrak{P}}}\right)=\prod_{\mathfrak{P}\mid p}N(\mathfrak{P})^{e_{\mathfrak{P}}}=\prod_{\mathfrak{P}\mid p}p^{e_{\mathfrak{P}}f_{\mathfrak{P}}}=p^{\left(\sum_{\mathfrak{P}\mid p}e_{\mathfrak{P}}f_{\mathfrak{P}}\right)}$

$|N_{K/\mathbb{Q}}(p)| = p^{[K:\mathbb{Q}]}$

Rmk. $\exists$ relative version: if $\mathbb{Q}\subset K\subset K'$, $[K':\mathbb{Q}]<\infty$, $\mathfrak{P}\in \mathrm{Spec}(\mathcal{O}_K)\setminus\{0\}$, then

$$\mathfrak{P}\mathcal{O}_{K'}=\prod_{\mathfrak{P}'\mid\mathfrak{P}}(\mathfrak{P}')^{e(\mathfrak{P}'\mid\mathfrak{P})}, \qquad [k(\mathfrak{P}'):k(\mathfrak{P})]=f(\mathfrak{P}'\mid\mathfrak{P}),$$

$$\sum_{\mathfrak{P}'\mid\mathfrak{P}} e(\mathfrak{P}'\mid\mathfrak{P})\,f(\mathfrak{P}'\mid\mathfrak{P}) = [K':K].$$

Chinese Remainder Thm: $\mathcal{O}_{K'}/\mathfrak{P}\mathcal{O}_{K'} \simeq \prod_{\mathfrak{P}'\mid\mathfrak{P}} \mathcal{O}_{K'}/\mathfrak{P}'^{e(\mathfrak{P}'\mid\mathfrak{P})}$

Discriminant and ramification

Note: If $\mathbb{K} \subset B$ are rings, $B = \mathbb{K}b_1 \oplus \cdots \oplus \mathbb{K}b_n$ and $K = \text{field}$,
$\forall x \in Nil(B) \quad (\exists\, m \geq 1 \;\; x^m = 0) \Rightarrow \forall y \in B \quad (xy)^m = 0$
$\Rightarrow$ $M(xy) \in M_n(\mathbb{K})$ is a nilpotent matrix $\quad (M(xy)^m = 0)$
$\Rightarrow$ $Tr_{B/\mathbb{K}}(xy) = Tr\, M(xy) = 0$.
In other words, $Nil(B) \neq 0 \Rightarrow$ $T : B \times B \longrightarrow K$ is degenerate.
$x, y \longmapsto Tr_{B/K}(xy)$.

Thm (Dedekind) A prime number p is ramified in $K/\mathbb{Q} \iff p \mid D_K$.

Pf. $(\mathcal{O}_K, +) = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, $(\mathcal{O}_K/p\mathcal{O}_K, +) = \mathbb{F}_p\overline{\alpha_1} \oplus \cdots \oplus \mathbb{F}_p\overline{\alpha_n}$
$D_K = D(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, $\overline{D_K} = D_K \pmod p = D(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = D_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p} \in \mathbb{F}_p$.

- If p is ramified in $K/\mathbb{Q} \Rightarrow$ $\mathcal{O}_K/p\mathcal{O}_K = \prod_{P \mid p} \mathcal{O}_K/P^{e_P}$, $\exists P \mid p \;\; e_P > 1$
$\Rightarrow$ $Nil(\mathcal{O}_K/P^{e_P}) \supset P/P^{e_P} \neq 0 \Longrightarrow$ $D_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p} = 0 \Rightarrow p \mid D_K$.
- If p is unramified in $K/\mathbb{Q} \Rightarrow$ $\mathcal{O}_K/p\mathcal{O}_K = \prod_{P \mid p} \underbrace{\mathcal{O}_K/P}_{k(P) \supset \mathbb{F}_p \text{ finite field}}$
$k(P)/\mathbb{F}_p$ is separable $\Rightarrow$ $D_{k(P)/\mathbb{F}_p} \neq 0 \in \mathbb{F}_p$
$\Rightarrow$ $D_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p} \neq 0 \in \mathbb{F}_p \Longrightarrow p \nmid D_K$.

Rmk. L field, $L \subset B$ ring, $\dim_L(B) < \infty \Rightarrow Spec(B) = Max(B) = \{m_1, \ldots, m_r\}$, $Nil(B) = m_1 \cap \cdots \cap m_r \overset{CRT}{\Longrightarrow} B/Nil(B) \simeq \prod_{i=1}^r \underbrace{B/m_i}_{\text{field } L_i,\ [L_i : L] < \infty}$
$\exists\, d \geq 1 \quad Nil(B)^d = 0 \overset{CRT}{\Rightarrow} B = B/Nil(B)^d \simeq \prod_{i=1}^r B/m_i^d$.
It follows that: $D_{B/L} \neq 0 \iff B \simeq \prod_{i=1}^r L_i$, L_i/L separable field extension.

Cor. (Minkowski) If $K \neq \mathbb{Q}$, then $\exists\, p$ ramified in $K/\mathbb{Q}$.

Thm (Kummer–Dedekind). Assume $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$; then $(\mathcal{O}_K : \mathbb{Z}[\alpha]) < \infty$.
Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. If $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$, then the factorisation of $p\mathcal{O}_K = \prod_i P_i^{e_i}$ mirrors the factorisation of $\overline{f} = f \pmod{p\mathbb{Z}[X]} = \prod_i \overline{g_i}^{e_i} \in \mathbb{F}_p[X]$: $\overline{g_i} \in \mathbb{F}[X]$ distinct, irreducible, monic, $f_i = \deg(\overline{g_i})$, $P_i = (p, g_i(\alpha))$ for any $g_i \in \mathbb{Z}[X]$ (monic) such that $\overline{g_i} = g_i \pmod{p\mathbb{Z}[X]}$.
Moreover, $\mathcal{O}_K/P_i \simeq \mathbb{F}_p[X]/(\overline{g_i})$, $N(P_i) = p^{f_i}$.

Rmk. As $disc(f) = D_{\mathbb{Z}[\alpha]/\mathbb{Z}} = D_K\,(\mathcal{O}_K : \mathbb{Z}[\alpha])^2$, it follows that $[p \nmid disc(f) \Rightarrow disc(\overline{f}) \neq 0 \in \mathbb{F}_p \Longrightarrow \forall i \;\; e_i = 1]$, which is a special case of Dedekind's Thm above.

Pf. Lemma: $X \subset Y$ abelian groups, (p prime) $p \nmid d = (Y:X) < \infty$. Then the map $\alpha: X/pX \longrightarrow Y/pY$ is an isomorphism.

Pf: $\mathrm{Ker}(\alpha) = \mathrm{Ker}(\alpha)[p]$, $\underbrace{\mathrm{Coker}(\alpha)}_{(Y/pY)/\mathrm{Im}(\alpha)} = \mathrm{Coker}(\alpha)[p]$.

Lagrange's Thm $\Rightarrow d(Y/X) = 0 \Rightarrow dY \subset X$.

$\mathrm{Ker}(\alpha) = (X \cap pY)/pX \subset pY/pX = (pY/pX)[d]$

$\mathrm{Coker}(\alpha) = Y/(X+pY) =$ quotient of $Y/X = (Y/X)[d]$.

Z any abelian group $\Rightarrow Z[p] \cap Z[d] = Z[\underbrace{\gcd(p,d)}_{1}] = \{0\}$, so if $Z = Z[p] = Z[d] \Rightarrow Z = 0$. This applies to $Z = \mathrm{Ker}(\alpha), \mathrm{Coker}(\alpha)$ $\Rightarrow \alpha$ is an isomorphism.

Back to Thm: $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha]) \overset{\text{Lemma}}{\Longleftrightarrow} \underbrace{\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]}_{\mathbb{Z}[X]/(f,p) = \mathbb{F}_p[X]/(\overline{f})} = \mathcal{O}_K/p\mathcal{O}_K$

As $\mathbb{Z}[X]/(f) \xrightarrow{\overline{g(X)} \longmapsto g(\alpha)} \mathbb{Z}[\alpha]$, we have

$$\simeq \prod_i \mathbb{F}_p[X]/(\overline{g_i}^{e_i}) \Longrightarrow \sum e_i f_i = \deg(f) = [K:\mathbb{Q}].$$

Moreover, if $P_i = p\mathcal{O}_K + g_i(\alpha)\mathcal{O}_K$, then

$$\mathcal{O}_K/P_i \overset{\text{Lemma}}{\xleftarrow{\sim}} \mathbb{Z}[\alpha]/(p\mathbb{Z}[\alpha] + g_i(\alpha)\mathbb{Z}[\alpha]) \xleftarrow{\sim} \mathbb{Z}[X]/(p, f, g_i)$$

$(f_i = \deg(\overline{g_i}))$ $\qquad \mathbb{F}_{p^{f_i}} = \mathbb{F}_p[X]/(\overline{g_i}) = \mathbb{Z}[X]/(p, g_i)$

$\Rightarrow P_i \in \mathrm{Spec}(\mathcal{O}_K) \setminus \{(0)\}$, $P_i \mid p$, $N(P_i) = p^{f_i}$.

As $\prod_i P_i^{e_i} \subset \prod_i (p, g_i(\alpha))^{e_i} \subset (p, \prod_i g_i(\alpha)^{e_i}) = (p, f(\alpha)) = p\mathcal{O}_K$

and $N(\prod_i P_i^{e_i}) = \prod_i p^{e_i f_i} = p^{[K:\mathbb{Q}]} = N(p\mathcal{O}_K) \Rightarrow \prod_i P_i^{e_i} = p\mathcal{O}_K$.

It remains to check that $P_i \neq P_j$ if $i \neq j$:

$i \neq j \Rightarrow \underbrace{(\overline{g_i}) + (\overline{g_j})}_{(\overline{g_i}, \overline{g_j})} = (1)$ in $\mathbb{F}_p[X] \Rightarrow (p, g_i, g_j) = (1)$ in $\mathbb{Z}[X]$

$\Rightarrow P_i + P_j = \mathcal{O}_K$.

Exercise. What are the relative versions of the above theorems (for $K \subset K'$)?

Rmk. Hermite proved the following finiteness theorem: There are only finitely many number fields K of a given degree $[K:\mathbb{Q}] = n$ that are unramified over $\mathbb{Q}$ outside a given finite set $\{p_1, \dots, p_k\}$ of prime numbers ($\Longleftrightarrow |D_K| = p_1^{m_1} \cdots p_k^{m_k}$ for some $m_i \geq 0$).

Def. If $[K:\mathbb{Q}]=n$ and if p is a prime number, $pO_K = \prod_{P \mid p} P^{e_P}$, we say that

p is totally ramified in $K/\mathbb{Q}$ if $pO_K = P^n$ ($\Rightarrow O_K/P = \mathbb{F}_p$)

p is inert in $K/\mathbb{Q}$ if $pO_K = P$ ($\Rightarrow O_K/P = \mathbb{F}_{p^n}$)

p splits completely in $K/\mathbb{Q}$ if $pO_K = P_1 \cdots P_n$, P_i distinct ($\Rightarrow O_K/P_i = \mathbb{F}_p$)

Ex. If $K=\mathbb{Q}(\alpha)$, $\alpha \in O_K$, if the minimal polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ of α over $\mathbb{Q}$ is an Eisenstein polynomial with respect to p ($\forall i\ p \mid a_i$, $p^2 \nmid a_0$) $\Rightarrow$ we know that $p \nmid (O_K : \mathbb{Z}[\alpha])$ $\Rightarrow$ the Kummer — Dedekind Thm applies:

$\overline{f} = X^n \in \mathbb{F}_p[X] \Rightarrow \overline{g_1} = X$, $e_1 = n$, $\deg(\overline{g_1}) = 1$,

$(p) = P^n$, $P = (p, \alpha)$, $O_K/P = \mathbb{F}_p$, $e_P = n$, $f_P = 1$

($\Rightarrow$ p is totally ramified in $\mathbb{Q}(\alpha)/\mathbb{Q}$).

Again, this admits a relative version for extensions L/K.

Normalised valuations on K ($[K:\mathbb{Q}] < \infty$)

Primes ($=$ "places") of K: finite primes $=$ non-zero prime ideals $P \subset O_K$ ($P \mid p$ prime number)

infinite primes $=$ embeddings $\sigma : K \hookrightarrow \mathbb{C}$ modulo complex conjugation

(notation: $\sigma \mid \infty$)

r_1 real primes $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ (notation: $K_\sigma = \mathbb{R}$)

r_2 complex primes $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2} : K \hookrightarrow \mathbb{C}$ ($\cdots$: $K_\sigma = \mathbb{C}$)

Def: For $\alpha \in K^*$ and a prime v of K we define

$$\|\alpha\|_v = \begin{cases} |\sigma(\alpha)|^{[K_\sigma : \mathbb{R}]} & \text{if } v = \sigma : K \hookrightarrow \mathbb{C} \\ N(P)^{-v_P(\alpha)} & \text{if } v = P \end{cases}$$

Thm. (1) $\forall$ prime number p $\quad \prod_{P \mid p} \|\alpha\|_P = p^{-v_p(N_{K/\mathbb{Q}}(\alpha))} = \|N_{K/\mathbb{Q}}(\alpha)\|_p$

$\forall \alpha \in K^*$

(2) $\prod_{\sigma \mid \infty} \|\alpha\|_\sigma = |N_{K/\mathbb{Q}}(\alpha)| = \|N_{K/\mathbb{Q}}(\alpha)\|_\infty$

(3) (The product formula) $\prod_w \|\alpha\|_w = \prod_{v \in P \cup \{\infty\}} \|N_{K/\mathbb{Q}}(\alpha)\|_v = 1$

Pf: (1) $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)| \Rightarrow v_p(N_{K/\mathbb{Q}}(\alpha)) = \sum_{P \mid p} v_p(\alpha) \underbrace{v_p(N(P))}_{f_P}$

(2) $N_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^{r_1} \sigma_j(\alpha) \prod_{k=1}^{r_2} \sigma_{r_1+k}(\alpha)\, \overline{\sigma_{r_1+k}(\alpha)}$.

(3) Follows from (1), (2) and the product formula over $\mathbb{Q}$.

Exercise (S-units) For any subset $S \subset \mathrm{Spec}(\mathcal{O}_K) \setminus \{0\}$, consider the subring $\mathcal{O}_{K,S} = \{\alpha \in K \mid \forall \mathfrak{p} \notin S \ \ v_{\mathfrak{p}}(\alpha) \geq 0\} \subset K$.

(Ex: $\mathcal{O}_{K,\emptyset} = \mathcal{O}_K$; $\mathcal{O}_{\mathbb{Q},\{p_1,\dots,p_r\}} = \mathbb{Z}\left[\frac{1}{p_1 \cdots p_r}\right]$).

(1) $\mathcal{O}_{K,S}$ is a Dedekind ring.

(2) $\mathrm{Cl}(\mathcal{O}_{K,S}) = \mathrm{Cl}(\mathcal{O}_K) / \{$the subgroup generated by the classes of all $\mathfrak{p} \in S\}$

(3) If $|S| < \infty$, then $\mathcal{O}_{K,S}^* / \mathcal{O}_K^* \simeq \mathbb{Z}^{|S|}$, $\mathcal{O}_{K,S}^* \simeq \mu(\mathcal{O}_K) \times \mathbb{Z}^{r_1+r_2-1+|S|}$.

[Hint: $\forall \mathfrak{p} \in S$ $\mathfrak{p}^{h_K}$ is principal]. (Ex: $\mathbb{Z}\left[\frac{1}{p_1 \cdots p_r}\right]^* = \{\pm 1\} \times p_1^{\mathbb{Z}} \times \cdots \times p_r^{\mathbb{Z}}$)

Prop.–Def. (Gauss's lemma for Dedekind rings)
Let $A =$ Dedekind ring, $K = \mathrm{Frac}(A)$. The content of $f \in A[X] \setminus \{0\}$ is the ideal $(0) \neq \mathrm{ct}(f) \subset A$ generated by the coefficients of f.

(1) $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)$

(2) If $f \in A[X]$, $g, h \in K[X]$ are monic and $f = gh \Rightarrow g, h \in A[X]$.

Pf (1) For each $\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{0\}$, $v_{\mathfrak{p}}(\mathrm{ct}(f)) = n_{\mathfrak{p}}$ is given by $\mathrm{ct}(f \in A_{\mathfrak{p}}[X]) = \pi^{n_{\mathfrak{p}}}$, where $A_{\mathfrak{p}} = \{\alpha \in K \mid v_{\mathfrak{p}}(\alpha) \geq 0\}$, $v_{\mathfrak{p}}(\pi) = 1$ (π = unique irreducible element of $A_{\mathfrak{p}}$). UFD

(2) $\exists\, \alpha, \beta \in A \setminus \{0\}$. $\alpha g, \beta h \in A[X]$. Then
$\mathrm{ct}(f) = (1)$, $\alpha \in \mathrm{ct}(\alpha g)$, $\beta \in \mathrm{ct}(\beta h)$ (since f, g, h are monic)

$\Rightarrow$ $\mathrm{ct}(\alpha g) \mid (\alpha)$, $\mathrm{ct}(\beta h) \mid (\beta)$
$\mathrm{ct}(\alpha g)\,\mathrm{ct}(\beta h) \overset{(1)}{=} \mathrm{ct}(\alpha\beta gh) = (\alpha\beta)$

$\Rightarrow$ $\mathrm{ct}(\alpha g) = (\alpha) \Rightarrow g \in A[X]$
$\mathrm{ct}(\beta h) = (\beta) \Rightarrow h \in A[X]$.

Exercise. Give an example (for example, for $A = \mathbb{Z}[i\sqrt{5}]$) that (2) is false if we do not assume f, g, h to be monic.

Exercise: Every number field K has a finite extension $L \supset K$ in which all ideals of $\mathcal{O}_K$ become principal: $\forall I \in I(\mathcal{O}_K) \quad I\mathcal{O}_L = (\beta) \subset L$.

Exercise: Let $K \subsetneq L$ be number fields. Show that: $(\mathcal{O}_L^* : \mathcal{O}_K^*) < \infty \iff$
$\iff K$ is totally real ($r_2 = 0$ for K) and $L = K(\sqrt{a})$, where $a \in K$, $\forall \sigma : K \hookrightarrow \mathbb{R}$ $\sigma(a) < 0$.

Exercise: (1) No prime number p is inert in $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

(2) The polynomial $f(x) = x^4 - 10x^2 + 1 = (x^2-5)^2 - 24 = (x^2+1)^2 - 12x^2 = (x^2-1)^2 - 8x^2$ is irreducible in $\mathbb{Q}[X]$, but $f \pmod p$ is reducible in $\mathbb{F}_p[X]$, for every prime number p.

(3) What is the relation between (1) and (2)?

Exercise: (1) Show that the polynomial $g(x) = x^3 - x + 2$ is irreducible in $\mathbb{Q}[X]$ and compute $\operatorname{disc}(g)$.

(2) Let $K = \mathbb{Q}(\alpha)$, where $g(\alpha) = 0$. Show that $(2) = 2\mathcal{O}_K = P^2 Q$, where the prime ideals P, Q are equal, respectively, to $P = (\alpha+1) = (\alpha-1)$ and $Q = (\alpha)$.

(3) Show that (3) is a prime ideal in $\mathcal{O}_K$.

(4) Show that $h_K = 1$ [Hint: use Minkowski's bound].

(5) Give an example of an explicit unit $u \in \mathcal{O}_K^* \setminus \{\pm 1\}$.

(6) Is $\mathcal{O}_K = \mathbb{Z}[\alpha]$?

$\mathfrak{P}$-adic numbers

Let $[K:\mathbb{Q}]=n$. For a prime number p,

$$p\mathcal{O}_K = \prod_{\mathfrak{P}\mid p} \mathfrak{P}^{e_{\mathfrak{P}}}, \qquad k(\mathfrak{P}) = \mathcal{O}_K/\mathfrak{P}, \quad [k(\mathfrak{P}):\mathbb{F}_p] = f_{\mathfrak{P}}, \quad \sum_{\mathfrak{P}\mid p} e_{\mathfrak{P}} f_{\mathfrak{P}} = n$$

The Chinese Remainder Theorem $\Rightarrow$

$$\forall r \geq 1 \quad \mathcal{O}_K/\mathfrak{p}^r\mathcal{O}_K \xrightarrow{\sim} \prod_{\mathfrak{P}\mid p} \mathcal{O}_K/\mathfrak{P}^{re_{\mathfrak{P}}}$$

$$\Rightarrow \underbrace{\varprojlim_r \mathcal{O}_K/\mathfrak{p}^r\mathcal{O}_K}_{\mathbb{Z}_p\alpha_1 \oplus \cdots \oplus \mathbb{Z}_p\alpha_n} \xrightarrow{\sim} \prod_{\mathfrak{P}\mid p} \left(\varprojlim_r \mathcal{O}_K/\mathfrak{P}^{re_{\mathfrak{P}}}\right) = \prod_{\mathfrak{P}\mid p} \underbrace{\left(\varprojlim_t \mathcal{O}_K/\mathfrak{P}^t\right)}_{\widehat{\mathcal{O}}_{K,\mathfrak{P}}}$$

if $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

the $\mathfrak{P}$-adic integers

For each $\mathfrak{P}\mid p$, $\widehat{\mathcal{O}}_{K,\mathfrak{P}}$ is an integral domain, with additive group of the form $(\widehat{\mathcal{O}}_{K,\mathfrak{P}}, +) \simeq \mathbb{Z}_p\beta_1 \oplus \cdots \oplus \mathbb{Z}_p\beta_{n_{\mathfrak{P}}}$, $n_{\mathfrak{P}} = e_{\mathfrak{P}} f_{\mathfrak{P}}$.

Moreover, $v_{\mathfrak{P}} : \widehat{\mathcal{O}}_{K,\mathfrak{P}} \longrightarrow \mathbb{N} \cup \{+\infty\}$

$$0 \longmapsto +\infty$$

$$(a_t)_{t\geq 1} \longmapsto \min\{t \geq 1 \mid a_t \not\equiv 0 \pmod{\mathfrak{P}^t}\} - 1$$

$a_t \in \mathcal{O}_K$, $a_{t+1} \equiv a_t \pmod{\mathfrak{P}^t}$

is a discrete valuation, $\{a \in \widehat{\mathcal{O}}_{K,\mathfrak{P}} \mid v_{\mathfrak{P}}(a) > 0\} = \mathfrak{P}\widehat{\mathcal{O}}_{K,\mathfrak{P}}$ is the unique non-zero prime ideal of $\widehat{\mathcal{O}}_{K,\mathfrak{P}}$ and

$$\widehat{\mathcal{O}}_{K,\mathfrak{P}} / (\mathfrak{P}\widehat{\mathcal{O}}_{K,\mathfrak{P}})^t \simeq \mathcal{O}_K/\mathfrak{P}^t \quad \text{for all } t \geq 1.$$

The fraction field $K_{\mathfrak{P}} = \mathrm{Frac}(\widehat{\mathcal{O}}_{K,\mathfrak{P}}) = \widehat{\mathcal{O}}_{K,\mathfrak{P}}[1/p]$ is the field of $\mathfrak{P}$-adic numbers, $[K_{\mathfrak{P}}:\mathbb{Q}_p] = n_{\mathfrak{P}} = e_{\mathfrak{P}} f_{\mathfrak{P}}$.

The Chinese Remainder theorem above can be written as

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} \prod_{\mathfrak{P}\mid p} \widehat{\mathcal{O}}_{K,\mathfrak{P}}, \text{ which implies that}$$

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{\mathfrak{P}\mid p} K_{\mathfrak{P}}.$$

Many questions involving ramification can be solved purely locally, in terms of $K_{\mathfrak{P}}$.

Terminology: $K_{\mathfrak{P}}$ is an example of a non-archimedean local field.

The different (Dedekind)

Recall: if $[K:\mathbb{Q}]=n$, the **trace form** $T: K\times K \to \mathbb{Q}$, $(\alpha,\beta)\mapsto Tr_{K/\mathbb{Q}}(\alpha\beta)$ is $\mathbb{Q}$-bilinear, symmetric, non-degenerate.

If $(\mathcal{O}_K,+)=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$, then $D_K=\det\left((T(\alpha_i,\alpha_j))_{1\le i,j\le n}\right)$.

Def. The **different of K** is the ideal $\mathfrak{D}_K\subset\mathcal{O}_K$ whose inverse is given by

$$\mathfrak{D}_K^{-1}=\{\alpha\in K \mid Tr_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)\subset\mathbb{Z}\}\supset\mathcal{O}_K.$$

Properties: (1) If $(\mathcal{O}_K,+)=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$, then $\mathfrak{D}_K^{-1}=\mathbb{Z}\alpha_1^*\oplus\cdots\oplus\mathbb{Z}\alpha_n^*$, where $T(\alpha_i,\alpha_j^*)=\delta_{ij}$ (the dual basis to $\{\alpha_i\}$ with respect to T is given by $\{\alpha_j^*\}$).

(2) Write $\alpha_i=\sum_{j=1}^{n}M_{ij}\alpha_j^*$, $M_{ij}\in\mathbb{Q}$. Then: $M_{ij}\in\mathbb{Z}$ $(\Leftarrow \mathfrak{D}_K^{-1}\supset\mathcal{O}_K)$, $T(\alpha_i,\alpha_j)=M_{ij}$,

$$|D_K|=|\det((M_{ij}))|=(\mathfrak{D}_K^{-1}:\mathcal{O}_K)=(\mathcal{O}_K:\mathfrak{D}_K^{-1})^{-1}=N(\mathfrak{D}_K^{-1})^{-1}=N(\mathfrak{D}_K).$$

(3) $\forall\, I\subset K$ fractional $\mathcal{O}_K$-ideal $I^*:=\{\alpha\in K \mid Tr_{K/\mathbb{Q}}(\alpha I)\subset\mathbb{Z}\}=I^{-1}\mathfrak{D}_K^{-1}$.

(4) If $\mathcal{O}_K=\mathbb{Z}[\beta]$, let $f(X)=(X-\beta_1)\cdots(X-\beta_n)\in\mathbb{Z}[X]$ be the minimal polynomial of β over $\mathbb{Q}$ ($\beta_1=\beta$). The elements $\alpha_i=\beta^{i-1}$, $\alpha_j'=\frac{\beta^{n-j}}{f'(\beta)}$ $(1\le i,j\le n)$ satisfy

$$Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j')=\begin{cases}\delta_{ij}, & \text{if } i\le j\\ \in\mathbb{Z}, & \text{if } i>j\end{cases}\Rightarrow \mathfrak{D}_K^{-1}=\mathbb{Z}\alpha_1^*\oplus\cdots\oplus\mathbb{Z}\alpha_n^*=\mathbb{Z}\alpha_1'\oplus\cdots\oplus\mathbb{Z}\alpha_n'=\frac{1}{f'(\beta)}\mathbb{Z}[\beta]$$

$\Rightarrow \mathfrak{D}_K=(f'(\beta))$ $\quad(\Rightarrow N(\mathfrak{D}_K)=|N_{K/\mathbb{Q}}(f'(\beta))|=|D_K|$, as in (2)).

Indeed, Lagrange's interpolation formula implies that

$$\forall k=1,\dots,n\quad X^k/f(X)=\delta_{kn}+\sum_{i=1}^{n}\frac{\beta_i^k}{f'(\beta_i)}\frac{1}{x-\beta_i}\Rightarrow X^k=\delta_{kn}f(X)+\sum_{i=1}^{n}\frac{\beta_i^k}{f'(\beta_i)}\frac{f(X)}{x-\beta_i}$$

For $k>n$, the same formula holds with δ_{kn} replaced by $g_k(X)=$ the polynomial part of $X^k/f(X)$ ($g_k\in\mathbb{Z}[X]$, $\deg(g_k)=k-n$) $\Rightarrow Tr_{K/\mathbb{Q}}(\beta^{k-1}/f'(\beta))=g_k(0)\in\mathbb{Z}$.

$$\Downarrow X=0$$

$$Tr_{K/\mathbb{Q}}(\beta^{k-1}/f'(\beta))=\sum_{i=1}^{n}\beta_i^{k-1}/f'(\beta_i)=\delta_{kn}$$

(5) **Dedekind**: if $p\mathcal{O}_K=\prod_{\mathfrak{P}\mid p}\mathfrak{P}^{e_{\mathfrak{P}}}$, then $v_{\mathfrak{P}}(\mathfrak{D}_K)\ge e_{\mathfrak{P}}-1$, with equality $\Leftrightarrow p\nmid e_{\mathfrak{P}}$.

In particular, $\mathfrak{P}\mid\mathfrak{D}_K\Leftrightarrow e_{\mathfrak{P}}>1$ ($\Leftrightarrow\mathfrak{P}$ is ramified in $K/\mathbb{Q}$).

(Hilbert gave an exact formula for $v_{\mathfrak{P}}(\mathfrak{D}_K)$).

(6) The **relative different** of $K\subset L$ $([L:\mathbb{Q}]<\infty)$ is the ideal $\mathfrak{D}_{L/K}\subset\mathcal{O}_L$ such that $\mathfrak{D}_{L/K}^{-1}=\{\alpha\in L \mid Tr_{L/K}(\alpha\mathcal{O}_L)\subset\mathcal{O}_K\}\supset\mathcal{O}_L$.

(7) **Transitivity formula**: $K\subset L\subset M\Rightarrow \mathfrak{D}_{M/K}=i(\mathfrak{D}_{L/K})\,\mathfrak{D}_{M/L}$

the ideal of $\mathcal{O}_M$ generated by $\mathfrak{D}_{L/K}$

(8) Again, if $\mathfrak{P}\in\mathrm{Max}(\mathcal{O}_K)$, $\mathfrak{Q}\in\mathrm{Max}(\mathcal{O}_L)$ and $\mathfrak{Q}\mid\mathfrak{P}$, then:

$\mathfrak{Q}\mid\mathfrak{D}_{L/K}\Leftrightarrow e(\mathfrak{Q}\mid\mathfrak{P})>1$ ($\Leftrightarrow\mathfrak{Q}$ is ramified in L/K)

$$\left(\mathfrak{P}\mathcal{O}_L=\prod_{\mathfrak{Q}\mid\mathfrak{P}}\mathfrak{Q}^{e(\mathfrak{Q}\mid\mathfrak{P})}\right)$$

(9) **Cor**: M/L is everywhere unramified $\Leftrightarrow |D_M|=|D_L|^{[M:L]}$