6. Ideals of rings of algebraic integers

Theorem 80 Let R be a commutative ring with identity and M an R-module. The following are equivalent:

(i) Every ascending chain $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ of submodules of M terminates (i.e., $\exists n_0 \in \mathbb{N} : N_{n_0} = N_{n_0+1} = N_{n_0+2} = \cdots$),

(ii) Every nonempty set $\mathcal{N}$ of submodules of M has a maximal element (with respect to set inclusion),

(iii) Every submodule N of M is finitely generated.

Proof: (i) $\Rightarrow$ (ii) Suppose there is a set $\mathcal{N} \neq \emptyset$ of submodules of M without a maximal element. As $\mathcal{N} \neq \emptyset$ there is an $N_1 \in \mathcal{N}$. As N_1 is not maximal there is a submodule $N_2 \in \mathcal{N}$ with $N_1 \subsetneq N_2$. Continuing like this we get an ascending chain $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$ of submodules of M which does not terminate.

(ii) $\Rightarrow$ (iii) Let $\mathcal{N} := \{F \mid F \text{ is a submodule of } N \text{ and } F \text{ is finitely generated}\}$. Then $\{0\} \in \mathcal{N}$ and thus $\mathcal{N} \neq \emptyset$. By assumption $\mathcal{N}$ has a maximal element F_0. By definition of $\mathcal{N}$ we know that F_0 is finitely generated, i.e., $\exists m_1, \ldots, m_n \in N : F_0 = \langle m_1, \ldots, m_n \rangle_R$. Suppose $F_0 \subsetneq N$. Then $\exists m_0 \in N \setminus F_0$ and $\langle m_0, m_1, \ldots, m_n \rangle_R$ would be a finitely generated submodule of N with the property $F_0 \subsetneq \langle m_0, m_1, \ldots, m_n \rangle_R$. This would contradict the maximality of F_0.

(iii) $\Rightarrow$ (i) If $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ is an ascending chain of submodules of M then $\bigcup_{i=1}^{\infty} N_i$ is also a submodule of M. (Let $m, n \in \bigcup_{i=1}^{\infty} N_i \Rightarrow \exists j, k \in \mathbb{N} : m \in N_j$ and $n \in N_k$ $\Rightarrow m+n \in N_{\max\{j,k\}} \subseteq \bigcup_{i=1}^{\infty} N_i$ and $\alpha m \in N_j \subseteq \bigcup_{i=1}^{\infty} N_i$ for all $\alpha \in R$.) By assumption $\bigcup_{i=1}^{\infty} N_i$ is finitely generated, i.e., $\exists m_1, \ldots, m_n \in M : \bigcup_{i=1}^{\infty} N_i = \langle m_1, \ldots, m_n \rangle_R$. We have that $\forall j \in \{1, \ldots, n\} \; \exists i_j \in \mathbb{N} : m_j \in N_{i_j}$. Set $I := \max\{i_1, \ldots, i_n\}$. Then $m_1, \ldots, m_n \in N_I$ and therefore $N_I \subseteq \bigcup_{i=1}^{\infty} N_i = \langle m_1, \ldots, m_n \rangle_R \subseteq N_I$, i.e., $\bigcup_{i=1}^{\infty} N_i = N_I$ and thus $N_I = N_{I+1} = N_{I+2} = \cdots$.

Definition: Let R be a commutative ring with identity. An R-module M which satisfies conditions (i)–(iii) in Theorem 80 is called a noetherian module [dt. noetherscher Modul]. The ring R is called a noetherian ring [dt. noetherscher Ring] if it is a noetherian R-module.

Corollary 81 Let R be a commutative ring with identity. The following are equivalent.

(i) Every ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals of R terminates,

(ii) Every nonempty set of ideals of R has a maximal element (with respect to set inclusion),

(iii) Every ideal of R is finitely generated.

Proof: Follows immediately from the definition and Theorem 80.

Theorem 82 (i) Every principal ideal domain R is a noetherian ring.

(ii) Let K be an algebraic number field. Then $\mathcal{O}_K$ is a noetherian ring.

Proof: (i) If I is an ideal of R then $\exists\, a \in R : I = (a)$, i.e., I is finitely generated.

(ii) By Theorem 61 $(\mathcal{O}_K, +)$ is a free abelian group of rank $[K:\mathbb{Q}]$. As $(I,+)$ is a subgroup of $(\mathcal{O}_K, +)$ Theorem 5 implies that $(I,+)$ is a free abelian group of rank $r \leq [K:\mathbb{Q}]$. I.e., there are $\alpha_1, \dots, \alpha_r \in I$ such that

$$I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_r \subseteq \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_r = (\alpha_1, \dots, \alpha_r) \subseteq I.$$

This shows that $I = (\alpha_1, \dots, \alpha_r)$ is finitely generated.

Remark: Hilbert's Basis Theorem [dt. Hilbertscher Basissatz] says that the polynomial ring $R[X_1, \dots, X_n]$ is noetherian if R is a noetherian ring. This result implies, e.g., that $\mathbb{Z}[X_1, \dots, X_n]$ is a noetherian ring and that $K[X_1, \dots, X_n]$ is a noetherian ring if K is a field.

Theorem 83 Let R be a noetherian integral domain. Then every $a \in R \setminus (R^* \cup \{0\})$ can be written as the product of finitely many irreducible elements of R.

Proof: Suppose there is a noetherian integral domain R and an $a \in R \setminus (R^* \cup \{0\})$ which cannot be written as a product of finitely many irreducible elements of R.

Let

$$\mathcal{A} := \{(a) \mid a \in R \setminus (R^* \cup \{0\}), a \text{ cannot be written as a product of finitely many irreducible elements of } R\}$$

By assumption $\mathcal{A} \neq \emptyset$. As R is noetherian $\mathcal{A}$ has a maximal element (μ). As μ cannot be irreducible there are $\beta, \gamma \in R \setminus R^*$: $\mu = \beta\gamma$. This implies $(\mu) \subseteq (\beta)$. If we had $(\mu) = (\beta)$ then μ and β would be associates and therefore $\gamma \in R^*$, which is a contradiction. Thus $(\mu) \subsetneq (\beta)$ and analogously $(\mu) \subsetneq (\gamma)$. As (μ) is maximal in $\mathcal{A}$ both β and γ can be written as products of finitely many irreducible elements of R, i.e., $\beta = \pi_1 \cdots \pi_k$ and $\gamma = \pi_{k+1} \cdots \pi_{k+\ell}$ where $\pi_1, \dots, \pi_{k+\ell}$ are irreducible. Therefore $\mu = \pi_1 \cdots \pi_{k+\ell}$ which is a contradiction.

Definition: Let D be an integral domain which satisfies the following three conditions:

1) D is a noetherian ring,

2) D is integrally closed,

3) Every prime ideal $P \neq (0)$ of D is a maximal ideal of D.

Then D is called a Dedekind domain [old: Dedekindring].

Remark: Condition 3) is a strong assumption. The polynomial ring $\mathbb{C}[X,Y]$ is an integral domain, noetherian (because of Hilbert's basis theorem) and integrally closed (by Theorem 52 as it is a unique factorization domain). However, in the chain $(0) \subsetneq (X) \subsetneq (X,Y)$ the three ideals (0), (X) and (X,Y) are all prime ideals. 7.12.2022

Theorem 84 Every principal ideal domain R is a Dedekind domain.

Proof: R is an integral domain by assumption and R is noetherian by Theorem 82 (i). As every principal ideal domain is a unique factorization domain, R is integrally closed by Theorem 52. We know from algebra that every prime ideal $P \neq (0)$ of R is a maximal ideal.

Examples: 1) $\mathbb{Z}$ is a Dedekind domain.

2) If K is a field then $K[X]$ is a Dedekind domain.

Lemma 85 Let K be an algebraic number field and $m \in \mathbb{Z} \setminus \{0\}$. Then $\mathcal{O}_K/(m)$ is a finite ring.

Proof: Let $\{\omega_1, \dots, \omega_n\}$ be an integral basis for K (with $n = [K:\mathbb{Q}]$). Then $\forall x \in \mathcal{O}_K \; \exists k_1, \dots, k_n \in \mathbb{Z}: x = k_1\omega_1 + \dots + k_n\omega_n$. For $1 \leq i \leq n$ let $k_i = q_i|m| + r_i$ with $0 \leq r_i < |m|$. Then

$$x = \sum_{i=1}^{n} k_i\omega_i = \sum_{i=1}^{n} (q_i|m| + r_i)\omega_i = \sum_{i=1}^{n} r_i\omega_i + |m| \sum_{i=1}^{n} q_i\omega_i \in \sum_{i=1}^{n} r_i\omega_i + (m),$$

i.e., every $x \in \mathcal{O}_K$ is in one of at most $|m|^n$ cosets of $\mathcal{O}_K/(m)$.

Theorem 86 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$.

(i) $\mathcal{O}_K/I$ is a finite ring,

(ii) $(I,+)$ is a free abelian group of rank $[K:\mathbb{Q}]$.

Proof: (i) Choose any $\alpha \in I \setminus \{0\}$ and let $m_{\mathbb{Q},\alpha}(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$. Then $a_0 \neq 0$. (If $n=1$ then $a_0 = -\alpha \neq 0$. If $n \geq 2$ then $a_0 \neq 0$ as $m_{\mathbb{Q},\alpha}$ is irreducible.) This implies $a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \dots - a_1\alpha \in (\alpha)$ and therefore $a_0\mathcal{O}_K = (a_0) \subseteq (\alpha) \subseteq I$. By Lemma 85 $\mathcal{O}_K/(a_0)$ is a finite ring. We know from

algebra that $I/(a_0)$ is an ideal of $\mathcal{O}_K/(a_0)$ and that $\mathcal{O}_K/I \cong (\mathcal{O}_K/(a_0))/(I/(a_0))$ (one of the isomorphism theorems for rings), which shows that $\mathcal{O}_K/I$ is finite.

(ii) Follows from (i) and Corollary 6.

Theorem 87 Let K be an algebraic number field. Then $\mathcal{O}_K$ is a Dedekind domain

Proof: $\mathcal{O}_K$ is an integral domain by Theorem 48, noetherian by Theorem 82 (ii) and integrally closed by Corollary 51. Let $P \neq (0)$ be a prime ideal of $\mathcal{O}_K$. By Theorem 86 (i) $\mathcal{O}_K/P$ is finite ring. As P is a prime ideal, $\mathcal{O}_K/P$ is an integral domain. As every finite integral domain is a field, $\mathcal{O}_K/P$ is a field. This implies that P is a maximal ideal.

Remark: A theorem by KRULL and AKIZUKI contains the following result: let R be a noetherian integral domain in which each prime ideal $P \neq (0)$ is maximal, Q the quotient field of R and K/Q a finite field extension. Then $\bar{R}^K$ is a Dedekind domain. Theorem 87 is a special case of this result.

Definition: Let R be a commutative ring with identity and I and J two ideals of R. Then set $I+J := \{\alpha+\beta \mid \alpha \in I, \beta \in J\}$.

Lemma 88 Let R be a commutative ring with identity and I, J and K ideals of R.

(i) $I+J$ is an ideal of R,

(ii) $I, J \subseteq I+J$,

(iii) $I+J = J+I$,

(iv) $I+(J+K) = (I+J)+K$.

Proof: See algebra

Definition: Let R be a commutative ring with identity and I, J two ideals of R. Then set $I \cdot J := \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n \mid \alpha_i \in I$ and $\beta_i \in J$ for $1 \leq i \leq n\}$.

Lemma 89 Let R be a commutative ring with identity, I, J, K and L ideals of R and $\alpha, \beta \in R$.

(i) $I \cdot J$ is an ideal of R,

(ii) $I \cdot J \subseteq I \cap J \subseteq I, J$,

(iii) $I \subseteq J \Rightarrow I \cdot K \subseteq J \cdot K$,

(iv) $I \subseteq J$ and $K \subseteq L \Rightarrow I \cdot K \subseteq J \cdot L$,

(v) $I \cdot J = J \cdot I$.

(vi) $I \cdot (J \cdot K) = (I \cdot J) \cdot K$,

(vii) $I \cdot (J + K) = I \cdot J + I \cdot K$ and $(I + J) \cdot K = I \cdot K + J \cdot K$,

(viii) $I \cdot R = R \cdot I = I \cdot (1) = (1) \cdot I = I$,

(ix) $(\alpha) \cdot (\beta) = (\alpha\beta)$ and $(\alpha) \cdot I = \alpha I = \{\alpha\beta \mid \beta \in I\}$.

Proof: Exercise

Theorem 90 Let R be a commutative ring with identity and P an ideal of R. The following are equivalent:

(i) P is a prime ideal (i.e., $P \subsetneq R$ and $\alpha \cdot \beta \in P \Rightarrow \alpha \in P \vee \beta \in P$),

(ii) $R \setminus P$ is a multiplicative subset of R (i.e., $1 \in R \setminus P$ and $\alpha\beta \in R \setminus P \ \forall \alpha, \beta \in R \setminus P$),

(iii) $P \subsetneq R$ and if I, J are two ideals of R then $I \cdot J \subseteq P \Rightarrow I \subseteq P \vee J \subseteq P$,

(iv) R/P is an integral domain

Proof: (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iv) is proved in algebra. Equivalence with (iii) is an exercise.

Definition: Let R be an integral domain, K its quotient field and $M \subseteq K$, $M \neq \emptyset$. Then M is called a fractional ideal of K [dt. gebrochenes Ideal von K] if M is an R-submodule of M and $\exists \alpha \in R \setminus \{0\} : \alpha M \subseteq R$.

Theorem 91 Let R be a noetherian integral domain, K its quotient field and $M \subseteq K$, $M \neq \emptyset$. The following are equivalent:

(i) M is a fractional ideal of K (i.e., M is an R-submodule of K and $\exists \alpha \in R \setminus \{0\} : \alpha M \subseteq R$),

(ii) There is an ideal I of R and an $\alpha \in R \setminus \{0\} : M = \alpha^{-1} I$,

(iii) There is an ideal I of R and an $x \in K : M = xI$,

(iv) M is a finitely generated R-submodule of K.

Proof: (i) $\Rightarrow$ (ii) Clearly αM is also an R-submodule of K (as $\alpha m + \alpha n = \alpha(m+n) \in \alpha M \ \forall m, n \in M$ and $x(\alpha m) = \alpha(xm) \in \alpha M \ \forall x \in R \ \forall m \in M$). Let $I := \alpha M$. Then I is an R-submodule of R, i.e., an ideal of R and $M = \alpha^{-1} I$.

(ii) $\Rightarrow$ (iii) Set $x = \alpha^{-1}$.

(iii) $\Rightarrow$ (iv) As R is noetherian, I is a finitely generated ideal, i.e. $\exists \alpha_1, \dots, \alpha_n \in I : I = R\alpha_1 + \dots + R\alpha_n$. This implies $M = xI = R(x\alpha_1) + \dots + R(x\alpha_n) = \langle x\alpha_1, \dots, x\alpha_n \rangle_R$, which shows that M is a finitely generated R-submodule of K.

(iv) $\Rightarrow$ (i) As M is finitely generated there are $x_1, \dots, x_n \in K : M = \langle x_1, \dots, x_n \rangle_R = Rx_1 + \dots + Rx_n$. As K is the quotient field of R, there is an $\alpha \in R \setminus \{0\} : \alpha x_1, \dots, \alpha x_n \in R$ and therefore $\alpha M = R(\alpha x_1) + \dots + R(\alpha x_n) \subseteq R$.

Example Let $R = \mathbb{Z}$ ($\Rightarrow K = \mathbb{Q}$). The fractional ideals of K are the sets of shape $\frac{m}{n}\mathbb{Z}$ (with $m \in \mathbb{Z}, n \in \mathbb{N}$): $\frac{m}{n}\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathbb{Q}$ (i.e., a subgroup of $(\mathbb{Q}, +)$) and $n \cdot \frac{m}{n}\mathbb{Z} = m\mathbb{Z} \subseteq \mathbb{Z}$. This shows that $\frac{m}{n}\mathbb{Z}$ is a fractional ideal of $\mathbb{Q}$.

If M is a fractional ideal of $\mathbb{Q}$, there is an ideal I of $\mathbb{Z}$ and an $n \in \mathbb{Z} \setminus \{0\}$ such that $M = \frac{1}{n} I$. As $\mathbb{Z}$ is a principal ideal domain, there is an $m \in \mathbb{Z}$: $I = m\mathbb{Z}$ and therefore $M = \frac{m}{n}\mathbb{Z} = \frac{(\operatorname{sgn} n) m}{|n|}\mathbb{Z}$.

Remarks: 1) Whether $M \subseteq K$ is a fractional ideal depends on R.

2) For this reason one often speaks of fractional ideals of R (instead of K), although a fractional ideal of R then need not be a subset of R.

3) An ideal of R is a fractional ideal of K and a fractional ideal M of K is an ideal of R if and only if $M \subseteq R$. For the sake of clarity ideals of R are often called integral ideals [dt. ganze Ideale]

4) The numbers α (in conditions (i) and (ii)) and x (in condition (iii)) and the ideal I (in conditions (ii) and (iii)) are not uniquely determined as

$$\alpha^{-1} I = (\alpha\beta)^{-1} (\beta I) \quad \forall \beta \in R \setminus \{0\}.$$

Definition Let D be a Dedekind domain and K its quotient field

1) If $\alpha, \beta \in D$, $\alpha \neq 0$ then $\alpha^{-1}(\beta) = \alpha^{-1}\beta D = \frac{\beta}{\alpha} D = \left\langle \frac{\beta}{\alpha} \right\rangle_D$ is called a principal fractional ideal of K [dt. gebrochenes Hauptideal von K].

2) An ideal I of D is also called an integral ideal of K

3) If M and N are fractional ideals of K, let $M + N = \{m + n \mid m \in M, n \in N\}$ and

$$M \cdot N = \left\{ \sum_{i=1}^{k} m_i \cdot n_i \;\middle|\; m_i \in M, n_i \in N \text{ for } 1 \leq i \leq k \right\}$$

12.12.2022

Lemma 92 Let D be a Dedekind domain and K its quotient field

(i) If M_1 and M_2 are fractional ideals of K then $M_1 + M_2$ and $M_1 \cdot M_2$ are fractional ideals of K,

(ii) If I, J are ideals of D and $\alpha, \beta \in D \setminus \{0\}$ then $\alpha^{-1} I + \beta^{-1} J = (\alpha\beta)^{-1}(\beta I + \alpha J)$ and $(\alpha^{-1} I)(\beta^{-1} J) = (\alpha\beta)^{-1}(I \cdot J)$,

(iii) If M_1, M_2 and M_3 are fractional ideals of K, the following identities hold.

$$M_1 + M_2 = M_2 + M_1,$$

$$M_1 + (M_2 + M_3) = (M_1 + M_2) + M_3,$$

$$M_1 \cdot M_2 = M_2 \cdot M_1,$$

$$M_1 \cdot (M_2 \cdot M_3) = (M_1 \cdot M_2) \cdot M_3,$$

$$M_1 \cdot (M_2 + M_3) = M_1 M_2 + M_1 M_3,$$

$$(M_1 + M_2) \cdot M_3 = M_1 M_3 + M_2 M_3,$$

$$M_1 \cdot D = D \cdot M_1 = M_1 \cdot (1) = (1) \cdot M_1 = M_1$$

(iv) If $\alpha_1,\alpha_2,\beta_1,\beta_2 \in D$, $\alpha_1\alpha_2 \neq 0$ then $\alpha_1^{-1}(\beta_1)\cdot\alpha_2^{-1}(\beta_2) = (\alpha_1\alpha_2)^{-1}\cdot(\beta_1\beta_2)$,

(v) If $\mathcal{F}_K := \{M \mid M \text{ is fractional ideal of } K, M \neq \{0\}\}$, then $(\mathcal{F}_K, \cdot)$ is a commutative monoid.

Proof: Exercise

Lemma 93 Let R be a noetherian commutative ring with identity and I (with $I \neq (0)$ and $I \neq R$) an ideal of R. Then there are prime ideals $P_1,\dots,P_k \neq (0)$ of R such that $P_1\cdots P_k \subseteq I$.

Proof: Suppose there are ideals $\neq (0)$ of R which do not have this property. Then $\mathcal{A} := \{I \mid I \neq (0)$ is an ideal and $P_1\cdots P_k \notin I$ for all prime ideals $P_1,\dots,P_k \neq (0)$ of $R\} \neq \emptyset$. As R is noetherian, $\mathcal{A}$ contains a maximal element J. Clearly J cannot be a prime ideal. Therefore, there are $\alpha,\beta \in R$ such that $\alpha\beta \in J$ but $\alpha,\beta \notin J$. Let $J_1 := J + (\alpha)$ and $J_2 := J + (\beta)$. Then $J \subsetneq J_1$ and $J \subsetneq J_2$ but $J_1J_2 = (J+(\alpha))(J+(\beta)) = J\cdot J + (\alpha)\cdot J + (\beta)J + (\alpha\beta) \subseteq J$. As J is maximal in $\mathcal{A}$ there are prime ideals $P_1,\dots,P_k \neq (0)$ and $Q_1,\dots,Q_\ell \neq (0)$ such that $P_1\cdots P_k \subseteq J_1$ and $Q_1\cdots Q_\ell \subseteq J_2$. This implies $P_1\cdots P_kQ_1\cdots Q_\ell \subseteq J_1J_2 \subseteq J$, which is a contradiction.

Definition: Let D be a Dedekind domain, K its quotient field and $I \neq (0)$ an ideal of D. Then let $I^{-1} := \{\alpha \in K \mid \alpha I \subseteq D\}$.

Lemma 94 Let D be a Dedekind domain, K its quotient field and $I, J \neq (0)$ ideals of D.

(i) I^{-1} is a fractional ideal of K,

(ii) If $I \subseteq J (\subseteq D)$ then $D \subseteq J^{-1} \subseteq I^{-1}$,

(iii) $I\cdot I^{-1}$ is an (integral) ideal of D.

Proof: (i) If $\alpha,\beta \in I^{-1}$ then $(\alpha+\beta)I \subseteq \alpha I + \beta I \subseteq D + D \subseteq D$ and if $\alpha \in I^{-1}$, $\gamma \in D$ then $(\gamma\alpha)I = \gamma(\alpha I) \subseteq \gamma D \subseteq D$, i.e., I^{-1} is a D-submodule of K. If $\alpha \in I \setminus \{0\}$ is arbitrary then $\alpha I^{-1} \subseteq D$ (by definition of I^{-1}). Therefore I^{-1} is a fractional ideal.

(ii) As I is an ideal of D we have $\alpha I \subseteq D$ $\forall \alpha \in D$ and therefore $D \subseteq I^{-1}$. If $I \subseteq J \subseteq D$ and $\alpha \in J^{-1}$ then $\alpha J \subseteq D$. Therefore $\alpha I \subseteq \alpha J \subseteq D$ and thus $\alpha \in I^{-1}$.

(iii) If $\alpha \in I$ and $\beta \in I^{-1}$ then $\alpha\beta \in D$ (by definition of I^{-1}) and therefore $I\cdot I^{-1} \subseteq D$. Because of (i) and Lemma 92 (i) $I\cdot I^{-1}$ is a fractional ideal and therefore an integral ideal.

Example: Let $D = \mathbb{Z}$ and $K = \mathbb{Q}$. If $I \neq (0)$ is an ideal of $\mathbb{Z}$, there is an $m \in \mathbb{N}$ such that $I = (m) = m\mathbb{Z}$ and $I^{-1} = \frac{1}{m}\mathbb{Z}$. (Let $\frac{k}{\ell} \in \mathbb{Q}$ with $k \in \mathbb{Z}$, $\ell \in \mathbb{N}$ and $\gcd(k,\ell) = 1$. Then $\frac{k}{\ell} \in I^{-1} \Rightarrow \frac{k}{\ell} m\mathbb{Z} \subseteq \mathbb{Z} \Rightarrow \frac{km}{\ell} \in \mathbb{Z} \Rightarrow \ell \mid (km) \Rightarrow \ell \mid m \Rightarrow \frac{k}{\ell} = \frac{1}{m}\cdot(k\frac{m}{\ell}) \in \frac{1}{m}\mathbb{Z}$, i.e., $I^{-1} \subseteq \frac{1}{m}\mathbb{Z}$. The inclusion $\frac{1}{m}\mathbb{Z} \subseteq I^{-1}$ is trivial.)

Lemma 95 Let D be a Dedekind domain, K its quotient field, $I \neq (0)$ an ideal of D and M a fractional ideal of K. If $I \cdot M \subseteq I$ then $M \subseteq D$.

Proof: As D is noetherian, I is finitely generated, i.e., there are $\omega_1, \dots, \omega_n \in I \setminus \{0\}$ such that $I = D\omega_1 + \dots + D\omega_n$. Let $\alpha \in M$. As $\alpha\omega_i \in I$ for $1 \leq i \leq n$ there are $\beta_{ij} \in D$ (with $1 \leq i,j \leq n$) such that $\alpha\omega_i = \sum_{j=1}^{n} \beta_{ij}\omega_j$ (for $1 \leq i \leq n$) and therefore $\sum_{j=1}^{n} (\alpha\delta_{ij} - \beta_{ij})\omega_j = 0$ (for $1 \leq i \leq n$).

As $(\omega_1, \dots, \omega_n) \neq (0, \dots, 0)$ the system of linear equations

$$\begin{pmatrix} \alpha-\beta_{11} & -\beta_{12} & \cdots & -\beta_{1n} \\ -\beta_{21} & \alpha-\beta_{22} & \cdots & -\beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\beta_{n1} & -\beta_{n2} & \cdots & \alpha-\beta_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

has a solution $\neq (0, \dots, 0)$. Therefore

$$\begin{vmatrix} \alpha-\beta_{11} & -\beta_{12} & \cdots & -\beta_{1n} \\ -\beta_{21} & \alpha-\beta_{22} & \cdots & -\beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\beta_{n1} & -\beta_{n2} & \cdots & \alpha-\beta_{nn} \end{vmatrix} = 0,$$ i.e., α is root of the monic polynomial

$$p(X) = \begin{vmatrix} X-\beta_{11} & -\beta_{12} & \cdots & -\beta_{1n} \\ -\beta_{21} & X-\beta_{22} & \cdots & -\beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\beta_{n1} & -\beta_{n2} & \cdots & X-\beta_{nn} \end{vmatrix} \in D[X].$$ As D is integrally closed we get $\alpha \in D$.

Theorem 96 Let D be a Dedekind domain, K its quotient field and $I \neq (0)$ an ideal of D. Then $I \cdot I^{-1} = D$.

Proof: 1st step: If $I \subsetneq D$ then $D \subsetneq I^{-1}$

We first show this claim for a maximal ideal P. Choose an $\alpha \in P \setminus \{0\}$. By Lemma 93 there are prime ideals $P_1, \dots, P_k \neq (0)$ such that $P_1 \cdots P_k \subseteq (\alpha)$ where k is chosen minimal. This means $P_1 \cdots P_k \subseteq (\alpha) \subseteq P$. As P is a prime ideal there is an $i \in \{1, \dots, k\}$ such that $P_i \subseteq P$. W.l.o.g let $P_1 \subseteq P$. As D is a Dedekind domain we get $P_1 = P$.

If $k = 1$ then $P_1 = (\alpha) = P$. Then $\alpha^{-1} \in P^{-1}$ but $\alpha^{-1} \notin D$ (as $\alpha^{-1} \in D$ would imply $\alpha \in D^*$ and thus $P = (\alpha) = D$, a contradiction).

If $k \geq 2$ then $P_2 \cdots P_k \not\subseteq (\alpha)$ as k was chosen minimal. Therefore, there is a $\beta \in P_2 \cdots P_k \setminus (\alpha)$. Thus $\beta P = \beta P_1 \subseteq P_1 \cdots P_k \subseteq (\alpha) \Rightarrow \beta\alpha^{-1}P \subseteq D \Rightarrow \beta\alpha^{-1} \in P^{-1}$. On the other hand $\beta\alpha^{-1} \notin D$ (as $\beta\alpha^{-1} \in D$ would imply $\beta \in \alpha D = (\alpha)$, a contradiction).

In both cases $P^{-1} \setminus D \neq \emptyset$ and therefore $D \subsetneq P^{-1}$ (because of Lemma 94(ii)).
If I is not maximal choose a maximal ideal P with $I \subseteq P$. Then $D \subsetneq P^{-1} \subseteq I^{-1}$.

2nd step: If P is a maximal ideal then $PP^{-1} = D$
By Lemma 94(iii) PP^{-1} is an (integral) ideal of D and satisfies $P = PD \subseteq PP^{-1} \subseteq D$.
As P is a maximal ideal either $PP^{-1} = P$ or $PP^{-1} = D$. If we had $PP^{-1} = P$ then $PP^{-1} \subseteq P$ and therefore $P^{-1} \subseteq D$ (because of Lemma 95) which contradicts the first step.

3rd step: If $I \neq (0)$ is an (integral) ideal of D then $I \cdot I^{-1} = D$
Suppose there are integral ideals $J \neq (0)$ with the property $J \cdot J^{-1} \subsetneq D$. Then we had $\mathfrak{A} := \{J \mid J \text{ is an ideal of } D, J \neq (0), J \cdot J^{-1} \subsetneq D\} \neq \emptyset$. As D is noetherian $\mathfrak{A}$ has a maximal element I. Let P be a maximal ideal with $I \subseteq P$. Then $D \subseteq P^{-1} \subseteq I^{-1}$ (because of Lemma 94(ii)) and therefore $I = I \cdot D \subseteq I \cdot P^{-1} \subseteq I \cdot I^{-1} \subseteq D$. This shows that $I \cdot P^{-1}$ is an integral ideal. If we had $I = I \cdot P^{-1}$ then $I \cdot P^{-1} \subseteq I$ and therefore $P^{-1} \subseteq D$ (because of Lemma 95), which contradicts the first step. Therefore $I \subsetneq I \cdot P^{-1}$ and (because I is maximal in $\mathfrak{A}$) $I \cdot P^{-1}(I \cdot P^{-1})^{-1} = D$. This implies $P^{-1}(IP^{-1})^{-1} \subseteq I^{-1}$ and thus $D = I \cdot P^{-1} \cdot (I \cdot P^{-1})^{-1} \subseteq I \cdot I^{-1} \subseteq D$ and $I \cdot I^{-1} = D$, which is a contradiction.

Theorem 97 Let D be a Dedekind domain, K its quotient field and
$\mathcal{F}_K = \{M \mid M \text{ is a fractional ideal of } K, M \neq \{0\}\}$. Then $(\mathcal{F}_K, \cdot)$ is an abelian group.

Proof: We stated in Lemma 95(v) that $(\mathcal{F}_K, \cdot)$ is a commutative monoid with identity element $D = (1)$. We proved in Theorem 96 that each integral ideal $I \neq (0)$ has an inverse $I^{-1} \in \mathcal{F}_K$. If $\alpha^{-1} I$ is a fractional ideal (with $\alpha \in D \setminus \{0\}$ and $I \neq (0)$ an integral ideal), then $(\alpha^{-1} I) \cdot (\alpha I^{-1}) = (\alpha^{-1}\alpha) I \cdot I^{-1} = D$.

14.12.2022

Theorem 98 Let D be a Dedekind domain. Then each (integral) ideal I of D (with $I \neq (0)$ and $I \neq D$) can be written as a product of prime ideals. This factorization is unique up to the order of the factors.
I.e., if I is an ideal of D (with $I \neq (0)$ and $I \neq D$), then there are prime ideals $P_1, \dots, P_k$ of D such that $I = P_1 \cdots P_k$. If also $I = Q_1 \cdots Q_\ell$ for some prime ideals $Q_1, \dots, Q_\ell$ of D then $k = \ell$ and there is a $\sigma \in S_k$ such that $Q_i = P_{\sigma(i)}$ for $1 \leq i \leq k$.

Proof: Existence: Suppose there are (integral) ideals J of D (with $J \neq (0)$ and $J \neq D$) which cannot be written as a product of prime ideals. Then we have
$\mathfrak{A} := \{J \mid J \text{ is an ideal of } D, J \neq (0), J \neq D, J \text{ cannot be written as a product of prime ideals}\} \neq \emptyset$.
As D is noetherian, $\mathfrak{A}$ has a maximal element I. Clearly I cannot be a prime ideal. Let P be a maximal ideal with $I \subseteq P$. We have $D \subseteq P^{-1}$ by Lemma 94(ii)

and therefore $I = I \cdot D \subseteq I \cdot P^{-1} \subseteq P \cdot P^{-1} = D$. If we had $I = I \cdot P^{-1}$ then $P^{-1} \subseteq D$ by Lemma 95, which would contradict the first step of the proof of Theorem 96. This implies $I \subsetneq I \cdot P^{-1}$. If we had $I \cdot P^{-1} = D$ then $I = P$ which is impossible. Therefore $I \cdot P^{-1} \subsetneq D$. As I is maximal in $\mathcal{A}$ there are prime ideals $P_1, \dots, P_k$ such that $I \cdot P^{-1} = P_1 \cdots P_k$ and thus $I = P \cdot P_1 \cdots P_k$, a contradiction.

Uniqueness: We use induction on k. $k=1$: $P_1 = Q_1 \cdots Q_\ell$ implies $Q_1 \cdots Q_\ell \subseteq P_1$. As P_1 is a prime ideal there is an $i \in \{1, \dots, \ell\}$ such that $Q_i \subseteq P_1$. W.l.o.g. let $Q_1 \subseteq P_1$. As D is a Dedekind domain we have $Q_1 = P_1$ and thus $D = P_1^{-1} Q_1 \cdots Q_\ell = Q_2 \cdots Q_\ell$. As $\ell \geq 2$ would imply $Q_2 \cdots Q_\ell \subseteq Q_2 \subsetneq D$ we get $\ell = 1$ and $P_1 = Q_1$.
Now assume the assertion has been proved for k and $P_1 \cdots P_{k+1} = Q_1 \cdots Q_\ell$. Then $Q_1 \cdots Q_\ell \subseteq P_{k+1}$. As P_{k+1} is a prime ideal there is an $i \in \{1, \dots, \ell\}$ such that $Q_i \subseteq P_{k+1}$. W.l.o.g. let $Q_\ell \subseteq P_{k+1}$. As D is a Dedekind domain we have $Q_\ell = P_{k+1}$ and therefore $P_1 \cdots P_k = (P_1 \cdots P_{k+1}) \cdot P_{k+1}^{-1} = (Q_1 \cdots Q_\ell) \cdot P_{k+1}^{-1} = Q_1 \cdots Q_{\ell-1}$. The induction hypothesis yields: $k = \ell - 1$ ($\Rightarrow k+1 = \ell$) and $\exists \sigma \in S_k : Q_j = P_{\sigma(j)}$ for $1 \leq j \leq k$. (It is easy to construct $\tau \in S_{k+1}$ such that $Q_j = P_{\sigma(j)}$ for $1 \leq j \leq k+1$ even if $i \neq \ell$.)

Remarks: 1) Theorems 97 and 98 imply (because of Theorem 87): If K is an algebraic number field, then the fractional ideals $\neq (0)$ of K are an abelian group. If I is an ideal of $\mathcal{O}_K$ (with $I \neq (0)$, $I \neq \mathcal{O}_K$) then I can be written as a product of prime ideals of $\mathcal{O}_K$. This factorization is unique up to the order of the factors.
2) Usually the factorization in Theorem 98 is written as $I = P_1^{n_1} \cdots P_k^{n_k}$ where $n_1, \dots, n_k \in \mathbb{N}$ and $P_1, \dots, P_k$ are pairwise different prime ideals. Often it is convenient to allow $n_i = 0$, letting $I^0 = D$.
3) Theorem 98 "saves" unique prime factorization. In the proof of Theorem 76 we used the equation $6 = 2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ to show that $\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \mathbb{Z}[i\sqrt{5}]$ is not a unique factorization domain. Rewriting this in terms of principal ideals we get $(6) = (2) \cdot (3) = (1+i\sqrt{5})(1-i\sqrt{5})$. One can check that there are pairwise different prime ideals P_1, P_2, P_3 such that

$$(6) = P_1^2 \cdot P_2 \cdot P_3, \quad (2) = P_1^2, \quad (3) = P_2 \cdot P_3, \quad (1+i\sqrt{5}) = P_1 \cdot P_2 \text{ and } (1-i\sqrt{5}) = P_1 \cdot P_3,$$

$$\text{i.e., } (2) \cdot (3) = P_1^2 \cdot P_2 P_3 \text{ and } (1+i\sqrt{5}) \cdot (1-i\sqrt{5}) = P_1 P_2 \cdot P_1 P_3.$$

4) One can show the following theorem: If R is an integral domain, then the following are equivalent:

(i) R is a Dedekind domain,

(ii) Each fractional ideal $M \neq (0)$ of the quotient field of R has an inverse M^{-1},

(iii) Each ideal I of R (with $I \neq (0), I \neq R$) can be written as a product of prime ideals of R.

Corollary 99 Let D be a Dedekind domain and K its quotient field. Each fractional ideal $M \neq \{0\}$ of K can be written as $M = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ where $P_1, \dots, P_k$ are pairwise different prime ideals of D and $\alpha_1, \dots, \alpha_k \in \mathbb{Z}$. This factorization is unique up to the order of the factors. (I.e., the group $\mathcal{F}_K$ is a free abelian group and the set of prime ideals $\neq (0)$ is a basis of $\mathcal{F}_K$.)

Proof: If $\alpha \in D \setminus \{0\}$ then $(\alpha)^{-1} = \alpha^{-1} D$. (Let $\beta \in \alpha^{-1} D$. Then $\exists \gamma \in D : \beta = \alpha^{-1}\gamma$ and $\beta(\alpha) = \alpha^{-1}\gamma(\alpha) \subseteq D \Rightarrow \beta \in (\alpha)^{-1}$, i.e., $\alpha^{-1} D \subseteq (\alpha)^{-1}$. Let $\beta \in (\alpha)^{-1}$. Then $\beta(\alpha) \subseteq D$ $\Rightarrow \beta\alpha \in D \Rightarrow \beta \in \alpha^{-1} D$, i.e., $(\alpha)^{-1} \subseteq \alpha^{-1} D$.)

Existence: By Theorem 91 there is an ideal I of D and an $\alpha \in D \setminus \{0\}$ such that $M = \alpha^{-1} I$. If $I = P_1^{\gamma_1} \dots P_k^{\gamma_k}$ and $(\alpha) = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ are the factorization of I and (α) into prime ideals (with $\gamma_i, \alpha_i \geq 0$ are integers for $1 \leq i \leq k$) then

$$M = \alpha^{-1} I = \alpha^{-1} D I = (\alpha)^{-1} I = P_1^{\gamma_1 - \alpha_1} \dots P_k^{\gamma_k - \alpha_k}.$$

Uniqueness: This factorization does not depend on I and α. Suppose we also have $M = \beta^{-1} J$ (where J is an ideal of D and $\beta \in D \setminus \{0\}$) and $J = P_1^{\delta_1} \dots P_k^{\delta_k}$ and $(\beta) = P_1^{\beta_1} \dots P_k^{\beta_k}$ are factorizations into prime ideals, then $\alpha^{-1} I = M = \beta^{-1} J$

$\Rightarrow (\beta) I = \beta D I = \beta I = \alpha J = \alpha D \cdot J = (\alpha) J \Rightarrow P_1^{\beta_1 + \gamma_1} \dots P_k^{\beta_k + \gamma_k} = P_1^{\alpha_1 + \delta_1} \dots P_k^{\alpha_k + \delta_k}$

$\Rightarrow \beta_i + \gamma_i = \alpha_i + \delta_i$ (for $1 \leq i \leq k$) $\Rightarrow \gamma_i - \alpha_i = \delta_i - \beta_i$ (for $1 \leq i \leq k$)

$\Rightarrow P_1^{\gamma_1 - \alpha_1} \dots P_k^{\gamma_k - \alpha_k} = P_1^{\delta_1 - \beta_1} \dots P_k^{\delta_k - \beta_k}$ $(= M)$.

Theorem 100 Let D be a Dedekind domain and I, J $(\neq (0))$ two ideals of D. Then the following are equivalent:

(i) $J \subseteq I$,

(ii) There is an ideal M of D such that $I \cdot M = J$,

(iii) If $I = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ and $J = P_1^{\beta_1} \dots P_k^{\beta_k}$ are the factorizations of I and J into prime ideals (where $\alpha_i, \beta_i \geq 0$ for $1 \leq i \leq k$) then $\alpha_i \leq \beta_i$ for $1 \leq i \leq k$

Proof: (i) $\Leftrightarrow$ (ii) $J \subseteq I \Leftrightarrow I^{-1} J \subseteq I^{-1} I = D \Leftrightarrow I^{-1} J$ is an (integral) ideal of D $\Leftrightarrow \exists$ ideal M of D such that $I^{-1} J = M \Leftrightarrow \exists$ ideal M of D such that $J = I \cdot M$.

(ii) $\Rightarrow$ (iii) Let $M = P_1^{\gamma_1} \cdots P_k^{\gamma_k}$ (with $\gamma_i \geq 0$ for $1 \leq i \leq k$). Then

$P_1^{\alpha_1+\gamma_1} \cdots P_k^{\alpha_k+\gamma_k} = IM = J = P_1^{\beta_1} \cdots P_k^{\beta_k} \Rightarrow \alpha_i + \gamma_i = \beta_i$ $(1 \leq i \leq k) \Rightarrow \alpha_i \leq \beta_i$ $(1 \leq i \leq k)$

(iii) $\Rightarrow$ (ii) Let $M := P_1^{\beta_1-\alpha_1} \cdots P_k^{\beta_k-\alpha_k}$. Then M is an ideal of D and $IM = J$.

Definition: Let D be a Dedekind domain and I, J $(\neq (0))$ two ideals of D. If I and J satisfy the three conditions of Theorem 100 one says that I divides J [old: I teilt J] and writes $I \mid J$.

9.1.2023

Corollary 101 Let D be a Dedekind domain and $P \neq (0)$ an ideal of D. Then the following are equivalent:

(i) P is a prime ideal,

(ii) $P \subsetneq D$ and $P \mid I \cdot J \Rightarrow P \mid I$ or $P \mid J$ for ideals I, J of D.

Proof: Condition (ii) is just a reformulation of condition (iii) in Theorem 90.

Corollary 102 Let D be a Dedekind domain and I, J $(\neq (0))$ two ideals of D. For an ideal G of D the following are equivalent:

(i) $G = I + J$,

(ii) $G \mid I$, $G \mid J$ and if $H \mid I$ and $H \mid J$ then $H \mid G$ (for ideals H of D),

(iii) If $I = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ and $J = P_1^{\beta_1} \cdots P_k^{\beta_k}$ (with $\alpha_i, \beta_i \geq 0$ for $1 \leq i \leq k$) then $G = P_1^{\min\{\alpha_1,\beta_1\}} \cdots P_k^{\min\{\alpha_k,\beta_k\}}$.

Proof: (i) $\Rightarrow$ (ii) $G = I + J \Rightarrow I \subseteq G$ and $J \subseteq G \Rightarrow G \mid I$ and $G \mid J$. If $H \mid I$ and $H \mid J$ then $I \subseteq H$ and $J \subseteq H \Rightarrow G = I + J \subseteq H \Rightarrow H \mid G$.

(ii) $\Rightarrow$ (i) $G \mid I$ and $G \mid J \Rightarrow I \subseteq G$ and $J \subseteq G \Rightarrow I + J \subseteq G$. Let $H := I + J$. Then $I \subseteq H$ and $J \subseteq H \Rightarrow H \mid I$ and $H \mid J \Rightarrow H \mid G \Rightarrow G \subseteq H = I + J$.

(ii) $\Rightarrow$ (iii) As $G \mid I$ implies $(0) \subsetneq I \subseteq G$ we see $G \neq (0)$. Let $G = P_1^{\gamma_1} \cdots P_k^{\gamma_k}$. As $G \mid P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ and $G \mid P_1^{\beta_1} \cdots P_k^{\beta_k}$ we get $\gamma_i \leq \alpha_i$ and $\gamma_i \leq \beta_i$ (for $1 \leq i \leq k$) by Theorem 100. Therefore $\gamma_i \leq \min\{\alpha_i, \beta_i\}$ (for $1 \leq i \leq k$). Let $H := P_1^{\min\{\alpha_1,\beta_1\}} \cdots P_k^{\min\{\alpha_k,\beta_k\}}$. Then $H \mid I$ and $H \mid J$ (by Theorem 100) $\Rightarrow H \mid G \overset{\text{Theorem 100}}{\Longrightarrow} \min\{\alpha_i, \beta_i\} \leq \gamma_i$ (for $1 \leq i \leq k$).

(iii) $\Rightarrow$ (ii) By Theorem 100 $P_1^{\min\{\alpha_1,\beta_1\}} \cdots P_k^{\min\{\alpha_k,\beta_k\}} \mid P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ and $P_1^{\min\{\alpha_1,\beta_1\}} \cdots P_k^{\min\{\alpha_k,\beta_k\}} \mid P_1^{\beta_1} \cdots P_k^{\beta_k}$, i.e., $G \mid I$ and $G \mid J$. If $H \mid I$ and $H \mid J$ (with $H = P_1^{\gamma_1} \cdots P_k^{\gamma_k}$) then $\gamma_i \leq \alpha_i$ and $\gamma_i \leq \beta_i$ (for $1 \leq i \leq k$) and therefore $\gamma_i \leq \min\{\alpha_i, \beta_i\}$ (for $1 \leq i \leq k$) which implies $G \mid H$.

Definition Let D be a Dedekind domain and I, J $(\neq (0))$ ideals of D. The ideal G of D

that satisfies the conditions from Corollary 102 is called the greatest common divisor of I and J [dt. größter gemeinsamer Teiler von I und J].

Remarks: 1) A special case of Corollary 102 is the relation

$$(a)+(b) = a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z} = (\gcd(a,b)) \quad \forall a,b \in \mathbb{Z}\setminus\{0\}.$$

2) Corollary 102 shows that two ideals I, J are "coprime" (i.e., if $I = P_1 \dots P_k$ and $J = Q_1 \dots Q_\ell$ then $P_i \neq Q_j$ for $1 \le i \le k$, $1 \le j \le \ell$) if and only if $I + J = D$.

Definition Let R be a commutative ring with identity. Two ideals I, J of R are called coprime [dt. coprim oder relativ prim] if $I + J = R$.

Corollary 103 Let D be a Dedekind domain and I, J ($\neq (0)$) two ideals of D. For an ideal L of D the following are equivalent:

(i) $L = I \cap J$,

(ii) $I \mid L$, $J \mid L$ and if $I \mid H$ and $J \mid H$ then $L \mid H$ (for ideals H of D),

(iii) If $I = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ and $J = P_1^{\beta_1} \dots P_k^{\beta_k}$ (with $\alpha_i, \beta_i \ge 0$ for $1 \le i \le k$) then

$$L = P_1^{\max\{\alpha_1,\beta_1\}} \dots P_k^{\max\{\alpha_k,\beta_k\}}.$$

Proof: (i) $\Rightarrow$ (ii) $L = I \cap J \Rightarrow L \subseteq I$ and $L \subseteq J \Rightarrow I \mid L$ and $J \mid L$. If $I \mid H$ and $J \mid H$ then $H \subseteq I$ and $H \subseteq J \Rightarrow H \subseteq I \cap J = L \Rightarrow L \mid H$.

(ii) $\Rightarrow$ (i) $I \mid L$ and $J \mid L \Rightarrow L \subseteq I$ and $L \subseteq J \Rightarrow L \subseteq I \cap J$. Let $H := I \cap J$. Then $H \subseteq I$ and $H \subseteq J \Rightarrow I \mid H$ and $J \mid H \Rightarrow L \mid H$ (i.e., $L \mid I \cap J$) $\Rightarrow I \cap J \subseteq L$.

(ii) $\Rightarrow$ (iii) We have $I \mid I \cdot J$ and $J \mid I \cdot J$ and therefore $L \mid I \cdot J$, i.e., $I \cdot J \subseteq L$. As $I \cdot J \neq (0)$ we get $L \neq (0)$. Let $L = P_1^{\gamma_1} \dots P_k^{\gamma_k}$. As $P_1^{\alpha_1} \dots P_k^{\alpha_k} \mid L$ and $P_1^{\beta_1} \dots P_k^{\beta_k} \mid L$ we get $\alpha_i \le \gamma_i$ and $\beta_i \le \gamma_i$ (for $1 \le i \le k$) by Theorem 100. Therefore $\max\{\alpha_i, \beta_i\} \le \gamma_i$ (for $1 \le i \le k$). Let $H := P_1^{\max\{\alpha_1,\beta_1\}} \dots P_k^{\max\{\alpha_k,\beta_k\}}$. Then $I \mid H$ and $J \mid H \Rightarrow L \mid H \overset{\text{Th. 100}}{\Longrightarrow} \gamma_i \le \max\{\alpha_i, \beta_i\}$ $(1 \le i \le k)$.

(iii) $\Rightarrow$ (ii) As $P_1^{\alpha_1} \dots P_k^{\alpha_k} \mid P_1^{\max\{\alpha_1,\beta_1\}} \dots P_k^{\max\{\alpha_k,\beta_k\}}$ and $P_1^{\beta_1} \dots P_k^{\beta_k} \mid P_1^{\max\{\alpha_1,\beta_1\}} \dots P_k^{\max\{\alpha_k,\beta_k\}}$ we see $I \mid L$ and $J \mid L$. If $I \mid H$ and $J \mid H$ with $H = P_1^{\gamma_1} \dots P_k^{\gamma_k}$ then $\alpha_i \le \gamma_i$ and $\beta_i \le \gamma_i$ (for $1 \le i \le k$) and therefore $\max\{\alpha_i, \beta_i\} \le \gamma_i$ (for $1 \le i \le k$) which implies $L \mid H$.
(Note that the condition $H \subseteq I$, $H \subseteq J \Rightarrow H \subseteq I \cap J$ is trivially fulfilled if $H = (0)$.)

Definition Let D be a Dedekind domain and I, J ($\neq (0)$) ideals of D. The ideal L of D that satisfies the conditions of Corollary 103 is called the least common multiple of I and J [dt. kleinstes gemeinsames Vielfaches von I und J].

Remark: A special case of Corollary 103 is the relation

$$(a)\cap(b) = (a\mathbb{Z})\cap(b\mathbb{Z}) = \operatorname{lcm}(a,b)\cdot\mathbb{Z} = (\operatorname{lcm}(a,b)) \quad \forall a,b\in\mathbb{Z}\setminus\{0\}.$$

Lemma 104 Let R be a commutative ring with identity and I,J ideals of R. Then the following are equivalent:

(i) I,J are coprime,

(ii) $\exists a\in I\ \exists b\in J: a+b=1$.

Proof: (i) $\Rightarrow$ (ii) $1\in R = I+J \Rightarrow \exists a\in I\ \exists b\in J: a+b=1$

(ii) $\Rightarrow$ (i) Let $a+b=1$ (with $a\in I$ and $b\in J$) and $x\in R$. Then $x = xa+yb \in I+J$, i.e., $R\subseteq I+J$ (and $I+J\subseteq R$ is trivial).

Lemma 105 Let R be a commutative ring with identity and I,J ideals of R. If I,J are coprime then $I\cdot J = I\cap J$.

Proof: The inclusion $IJ\subseteq I\cap J$ is contained in Lemma 89 (ii). The other inclusion follows from

$$I\cap J = (I\cap J)\cdot R = (I\cap J)\cdot(I+J) \overset{\text{Lemma 89 (v),(vii)}}{=} \underbrace{I\cdot(I\cap J)}_{\subseteq J} + \underbrace{(I\cap J)\cdot J}_{\subseteq I} \overset{\text{Lemma 89 (iv)}}{\subseteq} I\cdot J.$$

Lemma 106 Let R be a commutative ring with identity and $I,J_1,\dots,J_n$ ideals of R. If I and J_i are coprime (for $1\le i\le n$) then I and $J_1\cdots J_n$ are coprime.

Proof: Induction on n. $n=1$ is trivial

$n=2$ By Lemma 104 $\exists a,a'\in I\ \exists b\in J_1,\exists c\in J_2: a+b = a'+c = 1$

$$\Rightarrow bc = (1-a)(1-a') = 1-a-a'+aa' \Rightarrow \underbrace{bc}_{\in J_1J_2} + \underbrace{(a+a'-aa')}_{\in I} = 1 \overset{\text{Lemma 104}}{\Longrightarrow} I, J_1J_2 \text{ are coprime}$$

Let I,J_i be coprime for $1\le i\le n+1$. By the induction hypothesis I and $J_1\cdots J_n$ are coprime. The case $n=2$ implies that I and $(J_1\cdots J_n)J_{n+1} = J_1\cdots J_{n+1}$ are coprime.

Lemma 107 Let R be a commutative ring with identity and $I_1,\dots,I_n$ ideals of R. If $I_1,\dots,I_n$ are pairwise coprime (i.e., $I_i+I_j = R$ for $1\le i,j\le n, i\ne j$) then $I_1\cdots I_n = I_1\cap\cdots\cap I_n$.

Proof: Induction on n. $n=1$ is trivial and $n=2$ was proved in Lemma 105.

Suppose now that $n\ge 2$ and that the assertion has been proved for n.

Let $J := I_1\cdots I_n = I_1\cap\cdots\cap I_n$. Lemma 106 implies that J, I_{n+1} are coprime and

Therefore $I_1\cdots I_{n+1} = J\cdot I_{n+1} \overset{\text{Lemma 105}}{=} J\cap I_{n+1} = (I_1\cap\cdots\cap I_n)\cap I_{n+1} = I_1\cap\cdots\cap I_{n+1}$.

Theorem 108 (Chinese remainder theorem [dt chinesischer Restsatz])

Let R be a commutative ring with identity, $I_1,\dots,I_n$ ideals of R and

$\varphi: R \to \prod_{i=1}^{n} (R/I_i)$, $\varphi(a) = (a+I_1,\dots,a+I_n)$.

(i) φ is surjective $\iff$ $I_1,\dots,I_n$ are pairwise coprime,

(ii) $\ker\varphi = \bigcap_{i=1}^{n} I_i$,

(iii) φ is injective $\iff \bigcap_{i=1}^{n} I_i = (0)$,

(iv) If $I_1,\dots,I_n$ are pairwise coprime, then $R/(I_1\cdots I_n) \cong R/I_1 \times\cdots\times R/I_n$.

Proof: (i) ($\Rightarrow$) We will check wlog that I_1, I_2 are coprime. As φ is surjective, there is an $a\in R$ such that $\varphi(a) = (1_{R/I_1}, 0_{R/I_2},\dots,0_{R/I_n}) \Rightarrow a+I_1 = 1+I_1$ and $a+I_2 = I_2$

$\Rightarrow 1-a\in I_1$ and $a\in I_2 \Rightarrow 1 = (1-a)+a \in I_1+I_2 \overset{\text{Lemma 104}}{\Longrightarrow} I_1, I_2$ are coprime.

($\Leftarrow$) We first show that there is an $a\in R$ such that $\varphi(a) = (1_{R/I_1}, 0_{R/I_2},\dots,0_{R/I_n})$.

By assumption $I_1+I_i = R$ (for $2\le i\le n$) and using Lemma 104 we get

$\forall i\in\{2,\dots,n\}\ \exists a_i\in I_1\ \exists b_i\in I_i : a_i+b_i = 1$. Let $a := b_2\cdots b_n$. Then

$a = \prod_{i=2}^{n}(1-a_i) \in 1+I_1$, i.e., $a+I_1 = 1+I_1$ and $a\in I_i$ for $2\le i\le n$. One can show

along the same lines $\forall i\in\{1,\dots,n\}\ \exists a_i\in R : \varphi(a_i) = (0_{R/I_1},\dots,0_{R/I_{i-1}}, 1_{R/I_i}, 0_{R/I_{i+1}},\dots,0_{R/I_n})$.

If $(x_1+I_1,\dots,x_n\in I_n)\in \prod_{i=1}^{n}(R/I_i)$ (with $x_1,\dots,x_n\in R$) then

$$\varphi\Big(\sum_{i=1}^{n} x_i a_i\Big) = \sum_{i=1}^{n}\varphi(x_i)\varphi(a_i) = \sum_{i=1}^{n}(x_i+I_1,\dots,x_i\in I_i,\dots,x_i+I_n)(I_1,\dots,I_{i-1},1+I_i,I_{i+1},\dots,I_n)$$

$$= \sum_{i=1}^{n}(I_1,\dots,I_{i-1},x_i+I_i,I_{i+1},\dots,I_n) = (x_1+I_1,\dots,x_n\in I_n).$$

(ii) Trivial.

(iii) Follows from (ii) by a result from algebra.

(iv) Using the first isomorphism theorem we get

$$R/(I_1\cdots I_n) \overset{\text{Lemma 107}}{=} R/(I_1\cap\cdots\cap I_n) \overset{\text{(ii)}}{=} R/\ker\varphi \cong \operatorname{Im}\varphi \overset{\text{(i)}}{=} R/I_1\times\cdots\times R/I_n$$

11.1.2023

Definition Let R be a commutative ring with identity, I an ideal of R and $a,b\in R$.

Then set $a\equiv b \pmod I$ $:\iff a-b\in I$.

Remark: If $R=\mathbb{Z}$ and $I\neq(0)$ is an ideal of R then $\exists m\in\mathbb{N}: I=(m)$ and we have

$a\equiv b \pmod I \iff a-b\in I \iff a-b\in(m) \iff m\mid(a-b) \iff a\equiv b \pmod m$.

Corollary 109 (Chinese Remainder Theorem) Let R be a commutative ring with identity, $I_1,\dots,I_n$ pairwise coprime ideals of R and $\alpha_1,\dots,\alpha_n \in R$. Then there is an $x \in R$ such that $x \equiv \alpha_i \pmod{I_i}$ for $1 \le i \le n$ and x is uniquely determined up to elements of $I_1 \cdots I_n$.

Proof: Let $\varphi : R \to \prod_{i=1}^{n} (R/I_i)$ be as in Theorem 108. Then φ is surjective and

$\exists \alpha \in R : (\alpha + I_1,\dots,\alpha + I_n) = \varphi(\alpha) = (\alpha_1 + I_1,\dots,\alpha_n \in I_n) \Rightarrow \alpha + I_i = \alpha_i + I_i$ (for $1 \le i \le n$)

$\Rightarrow \alpha - \alpha_i \in I_i$ (for $1 \le i \le n$) $\Rightarrow \alpha \equiv \alpha_i \pmod{I_i}$ (for $1 \le i \le n$).

If $\varphi(\alpha) = \varphi(\beta) = (\alpha_1 + I_1,\dots,\alpha_n + I_n)$ then $\varphi(\alpha - \beta) = \varphi(\alpha) - \varphi(\beta) = (I_1,\dots,I_n)$, i.e.,

$\alpha - \beta \in \ker\varphi = I_1 \cdots I_n$ (and $\alpha - \beta \in I_1 \cdots I_n = \ker\varphi$ implies $\varphi(\alpha) = \varphi(\beta)$).

Definition Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$. Then $N(I) := |\mathcal{O}_K / I|$ is called the norm of I [dt. Norm von I].

Remark: By Theorem 86 $N(I) \in \mathbb{N}$ and $N(I) > 1$ if $I \subsetneq \mathcal{O}_K$.

Theorem 110 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$. If $\{\alpha_1,\dots,\alpha_n\}$ is a $\mathbb{Z}$-basis of I (with $n = [K:\mathbb{Q}]$) (which exists because of Theorem 86) then

$$N(I) = \sqrt{\tfrac{1}{d_K} \Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)}.$$

Proof: As $\{\alpha_1,\dots,\alpha_n\}$ is linearly independent over $\mathbb{Q}$, it is a basis of K as a $\mathbb{Q}$-vector space.

Let $\{\omega_1,\dots,\omega_n\}$ be an integral basis for K and $\alpha_i = \sum_{j=1}^{n} c_{ij}\omega_j$ (with $c_{ij} \in \mathbb{Z}$ for $1 \le i,j \le n$).

Set $C := (c_{ij})_{1 \le i,j \le n}$. By Corollary 6 $N(I) = |\mathcal{O}_K / I| = |\det C|$ (> 0) and by Lemma 3-1

$$\Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n) = (\det C)^2 \Delta_{K/\mathbb{Q}}(\omega_1,\dots,\omega_n) = (\det C)^2 d_K \ (\neq 0)$$

$$\Rightarrow (\det C)^2 = \tfrac{1}{d_K} \Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n) \Rightarrow N(I) = |\det C| = \sqrt{\tfrac{1}{d_K} \Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)}.$$

Theorem 111 Let K be an algebraic number field and $\alpha \in \mathcal{O}_K \setminus \{0\}$. Let $I := (\alpha) = \alpha\mathcal{O}_K$, i.e., I is the principal ideal generated by α. Then $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$.

Proof: Let $\{\omega_1,\dots,\omega_n\}$ be an integral basis for K (with $n = [K:\mathbb{Q}]$). Then $\{\alpha\omega_1,\dots,\alpha\omega_n\}$ is a $\mathbb{Z}$-basis of I. ($\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n \Rightarrow (\alpha) = \alpha\mathcal{O}_K = \mathbb{Z}\alpha\omega_1 + \cdots + \mathbb{Z}\alpha\omega_n$, i.e.,

$\langle \alpha\omega_1,\dots,\alpha\omega_n \rangle_{\mathbb{Z}} = (\alpha)$. If $k_1,\dots,k_n \in \mathbb{Z}$ and $\sum_{i=1}^{n} k_i \alpha\omega_i = 0 \Rightarrow \alpha \sum_{i=1}^{n} k_i\omega_i = 0 \Rightarrow \sum_{i=1}^{n} k_i\omega_i = 0$

$\Rightarrow k_1 = \cdots = k_n = 0$.) If $\sigma_i : K \hookrightarrow \mathbb{C}$ (with $1 \le i \le n$) are the different homomorphisms with $\sigma_i|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ then

$$\Delta_{K/\mathbb{Q}}(\alpha\omega_1,\dots,\alpha\omega_n) = \begin{vmatrix} \sigma_1(\alpha\omega_1) & \cdots & \sigma_1(\alpha\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha\omega_n) & \cdots & \sigma_n(\alpha\omega_n) \end{vmatrix}^2 = \begin{vmatrix} \sigma_1(\alpha)\sigma_1(\omega_1) & \cdots & \sigma_1(\alpha)\sigma_n(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha)\sigma_n(\omega_n) & \cdots & \sigma_n(\alpha)\sigma_n(\omega_n) \end{vmatrix}^2$$

$$= \left(\sigma_1(\alpha)\cdots\sigma_n(\alpha)\right)^2 \begin{vmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{vmatrix}^2 = \left(N_{K/\mathbb{Q}}(\alpha)\right)^2 \cdot \Delta_{K/\mathbb{Q}}(\omega_1,\dots,\omega_n) = \left(N_{K/\mathbb{Q}}(\alpha)\right)^2 \cdot d_K$$

and therefore

$$N(I) \overset{\text{Th 110}}{=} \sqrt{\frac{\Delta_{K/\mathbb{Q}}(\alpha\omega_1,\dots,\alpha\omega_n)}{d_K}} = \sqrt{\left(N_{K/\mathbb{Q}}(\alpha)\right)^2} = \left|N_{K/\mathbb{Q}}(\alpha)\right|.$$

Lemma 112 Let K be an algebraic number field and $P \neq (0)$ a prime ideal of $\mathcal{O}_K$. Then $(P^n/P^{n+1}, +) \cong (\mathcal{O}_K/P, +)$ $\forall n \geq 1$.

Proof: We have $P^{n+1} \subsetneq P^n$. ($P^{n+1} = P^n \cdot P \subseteq P^n$ and $P^{n+1} \neq P^n$ because of the unique factorization of ideals into prime ideals.) There is no integral ideal I such that $P^{n+1} \subsetneq I \subsetneq P^n$. (Suppose $P^{n+1} \subseteq I \subseteq P^n \Rightarrow P = P^{n+1} \cdot P^{-n} \subseteq I \cdot P^{-n} \subseteq P^n \cdot P^{-n} = \mathcal{O}_K \Rightarrow I \cdot P^{-n} = P$ or $I \cdot P^{-n} = \mathcal{O}_K$ $\Rightarrow I = P^{n+1}$ or $I = P^n$.) Choose $\alpha \in P^n \setminus P^{n+1}$. Then $P^{n+1} \subsetneq P^{n+1} + (\alpha) \subseteq P^n$ and thus $P^{n+1} + (\alpha) = P^n$. Consider the map $\varphi : (\mathcal{O}_K, +) \to (P^n/P^{n+1}, +)$, $\varphi(x) = \alpha x + P^{n+1}$

- $\alpha \in P^n \Rightarrow \alpha x \in P^n$ $\forall x \in \mathcal{O}_K \Rightarrow \varphi(x) = \alpha x + P^{n+1} \in P^n/P^{n+1}$ $\forall x \in \mathcal{O}_K$
- φ is a group homomorphism as it is the composition of the two group homomorphisms $(\mathcal{O}_K, +) \to (P^n, +)$, $x \mapsto \alpha x$ and $(P^n, +) \to (P^n/P^{n+1}, +)$, $y \mapsto y + P^{n+1}$
- φ is surjective because of $(\alpha) + P^{n+1} = P^n$
- $\ker\varphi = P$: Clearly $P \subseteq \ker\varphi$ ($x \in P \Rightarrow \alpha x \in P^n \cdot P = P^{n+1} \Rightarrow \varphi(x) = \alpha x + P^{n+1} = P^{n+1}$) $\ker\varphi$ is an $\mathcal{O}_K$-module ($x \in \ker\varphi \Rightarrow \varphi(x) = P^{n+1} \Rightarrow \alpha x + P^{n+1} = P^{n+1} \Rightarrow \alpha x \in P^{n+1}$ $\Rightarrow \alpha x y \in P^{n+1}$ $\forall y \in \mathcal{O}_K \Rightarrow xy \in \ker\varphi$ $\forall y \in \mathcal{O}_K$). An $\mathcal{O}_K$-submodule of $\mathcal{O}_K$ is an integral ideal, i.e., $\ker\varphi$ is an ideal of $\mathcal{O}_K$. As P is a maximal ideal we have $\ker\varphi = P$ or $\ker\varphi = \mathcal{O}_K$. If $\ker\varphi = \mathcal{O}_K$ then $P^n/P^{n+1} = \operatorname{Im}\varphi \cong \mathcal{O}_K/\ker\varphi = \{0\}$ because of the first isomorphism theorem, which contradicts $P^{n+1} \subsetneq P^n$. Therefore $\ker\varphi = P$ and the assertion follows from the first isomorphism theorem.

Lemma 113 Let K be an algebraic number field and $P \neq (0)$ a prime ideal of $\mathcal{O}_K$. Then $N(P^n) = N(P)^n$ $\forall n \geq 1$.

Proof: Induction on n. $n=1$ is trivial. As the map $\varphi: \mathcal{O}_K/\mathfrak{p}^{n+1} \to \mathcal{O}_K/\mathfrak{p}^n$, $\varphi(x+\mathfrak{p}^{n+1}) = x+\mathfrak{p}^n$ is an epimorphism (of rings) with $\ker\varphi = \mathfrak{p}^n/\mathfrak{p}^{n+1}$, the third isomorphism theorem implies $(\mathcal{O}_K/\mathfrak{p}^{n+1})/(\mathfrak{p}^n/\mathfrak{p}^{n+1}) \cong \mathcal{O}_K/\mathfrak{p}^{n+1}$. Therefore

$$N(\mathfrak{p}^{n+1}) = |\mathcal{O}_K/\mathfrak{p}^{n+1}| = |\mathcal{O}_K/\mathfrak{p}^n| \cdot |\mathfrak{p}^n/\mathfrak{p}^{n+1}| \overset{\text{Lemma 112}}{=} N(\mathfrak{p}^n) \cdot |\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})^n \cdot N(\mathfrak{p}) = N(\mathfrak{p})^{n+1}$$

Lemma 114 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$. If $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ is the factorization of I into prime ideals, then $N(I) = N(\mathfrak{p}_1)^{\alpha_1} \cdots N(\mathfrak{p}_k)^{\alpha_k}$.

Proof: The ideals $\mathfrak{p}_1^{\alpha_1}, \dots, \mathfrak{p}_k^{\alpha_k}$ are pairwise coprime (because of Corollary 102). Theorem 108 implies

$$N(I) = |\mathcal{O}_K/I| = |\mathcal{O}_K/\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}| = |\mathcal{O}_K/\mathfrak{p}_1^{\alpha_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k^{\alpha_k}|$$

$$= |\mathcal{O}_K/\mathfrak{p}_1^{\alpha_1}| \cdots |\mathcal{O}_K/\mathfrak{p}_k^{\alpha_k}| = N(\mathfrak{p}_1^{\alpha_1}) \cdots N(\mathfrak{p}_k^{\alpha_k}) \overset{\text{Lemma 113}}{=} N(\mathfrak{p}_1)^{\alpha_1} \cdots N(\mathfrak{p}_k)^{\alpha_k}$$

Theorem 115 Let K be an algebraic number field and $I, J \neq (0)$ two ideals of $\mathcal{O}_K$. Then $N(I \cdot J) = N(I) \cdot N(J)$

Proof: Let $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ and $J = \mathfrak{Q}_1^{\beta_1} \cdots \mathfrak{Q}_\ell^{\beta_\ell}$ be the factorizations of I and J into prime ideals. Then $IJ = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k} \mathfrak{Q}_1^{\beta_1} \cdots \mathfrak{Q}_\ell^{\beta_\ell}$ and

$$N(IJ) = N(\mathfrak{p}_1)^{\alpha_1} \cdots N(\mathfrak{p}_k)^{\alpha_k} N(\mathfrak{Q}_1)^{\beta_1} \cdots N(\mathfrak{Q}_\ell)^{\beta_\ell} = N(I)N(J).$$

(Note that the first equation is also true if $\mathfrak{p}_i = \mathfrak{Q}_j$ for some $1 \le i \le k$, $1 \le j \le \ell$.)

Theorem 116 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$.

(i) If $N(I)$ is a prime, then I is a prime ideal of $\mathcal{O}_K$,

(ii) $N(I) \in I$, i.e. $I \mid (N(I))$ (where $(N(I)) = N(I)\mathcal{O}_K$ denotes the principal ideal generated by $N(I)$).

(iii) If I is a prime ideal of $\mathcal{O}_K$, then there is a uniquely determined prime p such that $I \mid (p)$ (where $(p) = p\mathcal{O}_K$) and $N(I) = p^f$ for some $f \in \{1, 2, \dots, [K:\mathbb{Q}]\}$.

Proof: (i) Let $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ be the factorization into prime ideals. Then $N(I) = N(\mathfrak{p}_1)^{\alpha_1} \cdots N(\mathfrak{p}_k)^{\alpha_k}$. As $N(I)$ is a prime we get $k=1$ and $\alpha_1 = 1$, i.e., $I = \mathfrak{p}_1$

(ii) $N(I) = |\mathcal{O}_K/I|$ implies $N(I) \cdot x + I = N(I)(x+I) = I \quad \forall x \in \mathcal{O}_K \Rightarrow N(I) \cdot x \in I \quad \forall x \in \mathcal{O}_K$

$\Rightarrow (N(I)) \subseteq I \quad (\Leftrightarrow I \mid (N(I)) \Leftarrow N(I) \in I$.

(iii) If $N(I) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (prime factorization in $\mathbb{Z}$) then $(N(I)) = (p_1)^{\alpha_1} \cdots (p_k)^{\alpha_k}$ (principle ideals in $\mathcal{O}_K$). Part (ii) implies $I \mid (p_1)^{\alpha_1} \cdots (p_k)^{\alpha_k}$. As I is a prime ideal, there is an $i \in \{1, \dots, k\}$: $I \mid (p_i)$, i.e., there is a prime p such that $I \mid (p)$. Suppose there are two different primes p, q such that $I \mid (p)$ and $I \mid (q)$. There are $x, y \in \mathbb{Z}$ such that $px + qy = 1$ and therefore $(p) + (q) = \mathcal{O}_K$. As $I \mid (p)$ and $I \mid (q)$ there are integral ideals J_1 and J_2 such that $(p) = IJ_1$ and $(q) = IJ_2$ $\Rightarrow \mathcal{O}_K = (p) + (q) = IJ_1 + IJ_2 = I(J_1 + J_2) \Rightarrow I \mid \mathcal{O}_K$, which is a contradiction. Therefore, there is exactly one prime p such that $I \mid (p)$.

This implies $N(I) \mid N((p))$ (in $\mathbb{Z}$) $\overset{\text{Th 111}}{\Rightarrow} N(I) \mid N_{K/\mathbb{Q}}(p) \Rightarrow N(I) \mid p^{[K:\mathbb{Q}]} \Rightarrow N(I) = p^f$ for some $f \in \{1, 2, \dots, [K:\mathbb{Q}]\}$.

Remark: The reverse of (i) is not true. Let, e.g., $K = \mathbb{Q}(i)$ (and therefore $\mathcal{O}_K = \mathbb{Z}[i]$). If $p \equiv 3 \pmod 4$ is a prime then p is a prime element of $\mathbb{Z}[i]$ (by Theorem 79). Therefore $(p) = p\mathbb{Z}[i]$ is a prime ideal of $\mathbb{Z}[i]$ but $N((p)) = |N_{\mathbb{Q}(i)/\mathbb{Q}}(p)| = p^2$.

Definition Let K be an algebraic number field and $P \neq (0)$ a prime ideal of $\mathcal{O}_K$. By Theorem 116 (iii) there is a uniquely determined prime p such that $P \mid (p)$ and $N(P) = p^f$ (with $1 \leq f \leq [K:\mathbb{Q}]$). Then one says that P lies over the prime p (or the prime ideal (p)) [dt. P liegt über p bzw. (p)]. The integer f is called the inertial degree of P over p [dt. der Trägheitsgrad von P über p]. 16.1.2023

Remark: As $\mathcal{O}_K$ is a Dedekind domain any prime ideal $P \neq (0)$ is a maximal ideal and therefore $\mathcal{O}_K/P$ a field with $N(P) = p^f$ elements. As clearly $(\mathcal{O}_K/P) = p$ it contains a prime subfield $F \cong \mathbb{Z}/p\mathbb{Z}$ and $f = [\mathcal{O}_K/P : F] = [\mathcal{O}_K/p : \mathbb{Z}/p\mathbb{Z}]$.

Theorem 117 Let K be an algebraic number field with $[K:\mathbb{Q}] = n$ and p a prime. If $(p) = p\mathcal{O}_K = P_1^{e_1} \cdots P_g^{e_g}$ (with pairwise different prime ideals $P_1, \dots, P_g$ of $\mathcal{O}_K$ and $e_1, \dots, e_g \in \mathbb{N}$) and $N(P_i) = p^{f_i}$ (for $1 \leq i \leq g$) then $e_1 f_1 + \cdots + e_g f_g = n$.

Proof: This follows from

$$p^n = N_{K/\mathbb{Q}}(p) = N((p)) = N(P_1^{e_1} \cdots P_g^{e_g}) = N(P_1)^{e_1} \cdots N(P_g)^{e_g} = (p^{f_1})^{e_1} \cdots (p^{f_g})^{e_g} = p^{e_1 f_1 + \cdots + e_g f_g}.$$

Definition: Keeping the notation of Theorem 117 the integer e_i is called the ramification index of P_i over p (or (p)) [dt. der Verzweigungsindex von P über p bzw. (p)].

Remarks: 1) Theorem 117 implies $g \leq n$.

2) The ramification index e of the prime ideal P over the prime p is the uniquely determined positive integer such that $P^e \mid (p)$ but $P^{e+1} \nmid (p)$. Clearly $e \leq n$.

3) If K is a quadratic number field, $g \in \{1, 2\}$ by the first remark. If p is a prime there are the following three possibilities:

- $g = 2 \Rightarrow (e_1, f_1) = (e_2, f_2) = (1, 1)$, i.e., $(p) = P_1 P_2$ where $P_1 \neq P_2$ are prime ideals and $N(P_1) = N(P_2) = p$ (p splits [dt. p ist zerlegt]),
- $g = 1$ and $(e_1, f_1) = (2, 1)$, i.e., $(p) = P^2$ where P is a prime ideal and $N(P) = p$ (p ramifies [dt. p ist verzweigt]),
- $g = 1$ and $(e_1, f_1) = (1, 2)$, i.e., $(p) = P$ is a prime ideal and $N(P) = p^2$ (p is inert [dt. p ist träge]).

4) Theorem 117 can be generalized to extensions L/K of algebraic number fields.

Example: Let $K = \mathbb{Q}(i)$. Using Theorem 79 we get:

- primes $p \equiv 1 \pmod 4$ split. If $p = a^2 + b^2 = (a+bi)(a-bi)$ then $(p) = (a+bi)(a-bi)$ where $(a+bi)$ and $(a-bi)$ are two different prime ideals of $\mathbb{Z}[i]$ with $N((a+bi)) = N((a-bi)) = p$,
- 2 ramifies as $(2) = (-i(1+i)^2) = (1+i)^2$ where $(1+i)$ is a prime ideal of $\mathbb{Z}[i]$ with $N((1+i)) = 2$,
- primes $p \equiv 3 \pmod 4$ are inert as (p) is a prime ideal of $\mathbb{Z}[i]$ with $N((p)) = p^2$.

Lemma 118 Let K be an algebraic number field and $P \neq (0)$ a prime ideal of $\mathcal{O}_K$ that lies over the prime p.

(i) $a + P = b + P \iff a \equiv b \pmod p \quad \forall a, b \in \mathbb{Z}$,

(ii) If $N(P) = p$ then $\mathcal{O}_K / P = \{a + P \mid a \in \mathbb{Z}, 0 \leq a < p\}$.

Proof: (i) $(\Rightarrow)$ $a + P = b + P \Rightarrow a - b \in P \Rightarrow (a-b) \subseteq P \Rightarrow P \mid (a-b) \Rightarrow N(P) \mid N((a-b))$
As $p \mid N(P)$ and $N((a-b)) = |a-b|^{[K:\mathbb{Q}]}$ we get $p \mid (a-b)$ and therefore $a \equiv b \pmod p$.
$(\Leftarrow)$ $a \equiv b \pmod p \Rightarrow p \mid (a-b) \Rightarrow (a-b) \subseteq (p) \Rightarrow (p) \mid (a-b)$. As $P \mid (p)$ we get $P \mid (a-b)$
$\Rightarrow (a-b) \subseteq P \Rightarrow a - b \in P \Rightarrow a + P = b + P$.

(ii) The assertion follows from (i) as $|\mathcal{O}_K / P| = N(P) = p$.

Theorem 119 Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and p a prime.

If $p > 2$ then: p ramifies if $p \mid d$,
p splits if $p \nmid d$ and $\left(\frac{d}{p}\right) = 1$,
p is inert if $p \nmid d$ and $\left(\frac{d}{p}\right) = -1$.

If $p = 2$ then: 2 ramifies if $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$,
2 splits if $d \equiv 1 \pmod 8$,
2 is inert if $d \equiv 5 \pmod 8$.

The ideal $(p) = p\mathcal{O}_K$ has the following factorizations into prime ideals:

If $p > 2$ then

$$(p) = \begin{cases} (p, \sqrt{d})^2 & \text{if } p \mid d, \\ (p, a + \sqrt{d})(p, a - \sqrt{d}) & \text{if } p \nmid d \text{ and } a \in \mathbb{Z} \text{ with } a^2 \equiv d \pmod p, \\ (p) & \text{if } p \nmid d \text{ and } \left(\frac{d}{p}\right) = -1. \end{cases}$$

If $p = 2$ then

$$(2) = \begin{cases} (2, \sqrt{d})^2 & \text{if } d \equiv 2 \pmod 4 \\ (2, 1 + \sqrt{d})^2 & \text{if } d \equiv 3 \pmod 4, \\ (2, \frac{1}{2}(1+\sqrt{d}))(2, \frac{1}{2}(1-\sqrt{d})) & \text{if } d \equiv 1 \pmod 8, \\ (2) & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

Proof: As d is squarefree we see $d \equiv 1, 2$ or $3 \pmod 4$.

1st case $p > 2$, $p \nmid d$ and $\left(\frac{d}{p}\right) = 1$, i.e., $\exists a \in \mathbb{Z} : a^2 \equiv d \pmod p$. Clearly $p \nmid a$ (as $p \nmid d$)
Let $P_1 := (p, a + \sqrt{d})$ and $P_2 := (p, a - \sqrt{d})$. Then

$P_1P_2 = (p, a+\sqrt{d})(p, a-\sqrt{d}) = (p^2, p(a+\sqrt{d}), p(a-\sqrt{d}), a^2-d) = (p)(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p})$

$\overset{(*)}{=} (p)\cdot(1) = (p)$

Here, the equation $(*)$ holds as $\gcd(2a, p) = 1$ implies that there are $x, y \in \mathbb{Z}$ such that $1 = px + 2ay = px + (a+\sqrt{d})y + (a-\sqrt{d})y \in (p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p})$.

We claim that $P_1, P_2 \neq \mathcal{O}_K$. Suppose $P_1 = \mathcal{O}_K \Rightarrow 1 \in P_1 \Rightarrow \exists \alpha, \beta \in \mathcal{O}_K : \alpha p + \beta(a+\sqrt{d}) = 1$

Applying $\sigma : K \to K, \sigma(r+s\sqrt{d}) = r - s\sqrt{d}$ (with $r, s \in \mathbb{Q}$) we get $\sigma(\alpha)p + \sigma(\beta)(a-\sqrt{d}) = 1$

$\Rightarrow 1 \in P_2 \Rightarrow P_2 = \mathcal{O}_K \Rightarrow (p) = P_1P_2 = \mathcal{O}_K^2 = \mathcal{O}_K$, a contradiction. For the same reason

$P_2 = \mathcal{O}_K$ is impossible.

As $p^2 = N_{K|\mathbb{Q}}(p) = N((p)) = N(P_1)N(P_2)$ we get $N(P_1) = N(P_2) = p$. By Theorem 116 (i)

P_1 and P_2 are prime ideals.

It remains to show that $P_1 \neq P_2$. Clearly $P_1 \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ and $p\mathbb{Z} \subseteq P_1 \cap \mathbb{Z}$

As $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ either $P_1 \cap \mathbb{Z} = p\mathbb{Z}$ or $P_1 \cap \mathbb{Z} = \mathbb{Z}$. As $P_1 \cap \mathbb{Z} = \mathbb{Z}$ would imply $1 \in P_1$ ($\Rightarrow P_1 = \mathcal{O}_K$) we see $P_1 \cap \mathbb{Z} = p\mathbb{Z}$. Now $P_1 = P_2$ would imply

$2a = (a+\sqrt{d}) + (a-\sqrt{d}) \in P_1 \cap \mathbb{Z} = p\mathbb{Z}$ and therefore $p \mid (2a)$, a contradiction

<u>2nd case</u> $p > 2$, $p \nmid d$ and $\left(\frac{d}{p}\right) = -1$. If we had $(p) = PQ$ for some prime ideals P, Q of $\mathcal{O}_K$ (where $P = Q$ is possible) we would get $p^2 = N_{K|\mathbb{Q}}(p) = N((p)) = N(P)N(Q)$ and therefore $N(P) = p$. As $\sqrt{d} \in \mathcal{O}_K$ Lemma 118 (ii) yields: $\exists\, c \in \mathbb{Z} : \sqrt{d} + P = c + P$

$\Rightarrow \sqrt{d} - c \in P \Rightarrow d - c^2 = (\sqrt{d}+c)(\sqrt{d}-c) \in P \Rightarrow d + P = c^2 + P \overset{\text{Lemma 118 (i)}}{\Longrightarrow} c^2 \equiv d \pmod{p}$

which contradicts $\left(\frac{d}{p}\right) = -1$. Therefore (p) is a prime ideal

<u>3rd case</u> $p > 2$ and $p \mid d$. Let $P = (p, \sqrt{d})$. Then

$P^2 = (p, \sqrt{d})(p, \sqrt{d}) = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, \frac{d}{p}) \overset{(*)}{=} (p)\cdot(1) = (p)$

(d is squarefree $\Rightarrow \gcd(p, \frac{d}{p}) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : 1 = px + \frac{d}{p}y \in (p, \sqrt{d}, \frac{d}{p}) \Rightarrow (*)$)

and $p^2 = N_{K|\mathbb{Q}}(p) = N((p)) = N(P)^2 \Rightarrow N(P) = p \overset{\text{Th 116 (i)}}{\Longrightarrow} P$ is a prime ideal

<u>4th case</u> $p = 2$ and $d \equiv 2 \pmod 4$. Let $P = (2, \sqrt{d})$. Then

$P^2 = (2, \sqrt{d})(2, \sqrt{d}) = (4, 2\sqrt{d}, d) = (2)(2, \sqrt{d}, \frac{d}{2}) \overset{(*)}{=} (2)(1) = (2)$

($d \equiv 2 \pmod 4 \Rightarrow \frac{d}{2} \equiv 1 \pmod 2 \Rightarrow \gcd(2, \frac{d}{2}) = 1$

$\Rightarrow \exists x, y \in \mathbb{Z} : 1 = 2x + \frac{d}{2}y \in (2, \sqrt{d}, \frac{d}{2}) \Rightarrow (*)$)

and $4 = N_{K|\mathbb{Q}}(2) = N((2)) = N(P)^2 \Rightarrow N(P) = 2 \overset{\text{Th 116 (i)}}{\Longrightarrow} P$ is a prime ideal

<u>5th case</u> $p = 2$ and $d \equiv 3 \pmod 4$. Let $P = (2, 1+\sqrt{d})$. As $1 - \sqrt{d} = 2 - (1+\sqrt{d})$

we see $P = (2, 1-\sqrt{d})$ and

$P^2 = (2, 1+\sqrt{d})(2, 1-\sqrt{d}) = (4, 2(1+\sqrt{d}), 2(1-\sqrt{d}), 1-d) = (2)(2, 1+\sqrt{d}, 1-\sqrt{d}, \frac{1-d}{2})$

$\overset{(*)}{=} (2)\cdot(1) = (2)$

$(d \equiv 3 \pmod 4) \Rightarrow \frac{1-d}{2} \equiv 1 \pmod 2 \Rightarrow \gcd(2, \frac{1-d}{2}) = 1$

$\Rightarrow \exists x, y \in \mathbb{Z} : 1 = 2x + \frac{1-d}{2} y \in (2, 1+\sqrt{d}, 1-\sqrt{d}, \frac{1-d}{2}) \Rightarrow (*))$

and $4 = N_{K|\mathbb{Q}}(2) = N((2)) = N(P)^2 \Rightarrow N(P) = 2 \xrightarrow{\text{Th 116 (i)}} P$ is a prime ideal

6th case $p = 2$ and $d \equiv 1 \pmod 8$. Let $P_1 = (2, \frac{1+\sqrt{d}}{2})$ and $P_2 = (2, \frac{1-\sqrt{d}}{2})$

(Note that $d \equiv 1 \pmod 8 \Rightarrow d \equiv 1 \pmod 4 \Rightarrow \frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$.) Then

$P_1 P_2 = (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) = (4, 1+\sqrt{d}, 1-\sqrt{d}, \frac{1-d}{4}) = (2)(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8}) \overset{(*)}{=} (2)(1) = (2)$

$(1 = \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} \in (2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8}) \Rightarrow (*))$

We claim that $P_1, P_2 \neq \mathcal{O}_K$. Suppose $P_1 = \mathcal{O}_K \Rightarrow 1 \in P_1 \Rightarrow \exists \alpha, \beta \in \mathcal{O}_K : 2\alpha + \frac{1+\sqrt{d}}{2}\beta = 1$

Applying $\sigma : K \to K$, $\sigma(r + s\sqrt{d}) = r - s\sqrt{d}$ (with $r, s \in \mathbb{Q}$) we get $2\sigma(\alpha) + \frac{1-\sqrt{d}}{2}\sigma(\beta) = 1$

$\Rightarrow 1 \in P_2 \Rightarrow P_2 = \mathcal{O}_K \Rightarrow (2) = P_1 P_2 = \mathcal{O}_K^2 = \mathcal{O}_K$, a contradiction. For the same reason

$P_2 = \mathcal{O}_K$ is impossible.

As $4 = N_{K|\mathbb{Q}}(2) = N((2)) = N(P_1) N(P_2)$ we get $N(P_1) = N(P_2) = 2$. By Theorem 116 (i)

P_1 and P_2 are prime ideals.

It remains to show that $P_1 \neq P_2$. Clearly $P_1 \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ and $2\mathbb{Z} \subseteq P_1 \cap \mathbb{Z}$

As $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ either $P_1 \cap \mathbb{Z} = 2\mathbb{Z}$ or $P_1 \cap \mathbb{Z} = \mathbb{Z}$. As $P_1 \cap \mathbb{Z} = \mathbb{Z}$ would

imply $1 \in P_1$ ($\Rightarrow P_1 = \mathcal{O}_K$) we see $P_1 \cap \mathbb{Z} = 2\mathbb{Z}$. Now $P_1 = P_2$ would imply

$1 = \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} \in P_1 \cap \mathbb{Z} = 2\mathbb{Z}$, a contradiction.

7th case $p = 2$ and $d \equiv 5 \pmod 8$. If we had $(2) = PQ$ for some prime ideals P, Q

of $\mathcal{O}_K$ (where $P = Q$ is possible) we would get $4 = N_{K|\mathbb{Q}}(2) = N((2)) = N(P) N(Q)$

and therefore $N(P) = 2$. As $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ Lemma 118 (ii) yields: $\exists a \in \mathbb{Z} : \frac{1+\sqrt{d}}{2} + P = a + P$

$\Rightarrow \frac{1+\sqrt{d}}{2} - a \in P \Rightarrow (1-a) - \frac{1-\sqrt{d}}{2} = (1-a) - (1 - \frac{1+\sqrt{d}}{2}) \in P \Rightarrow \frac{1-\sqrt{d}}{2} + P = 1 - a + P$

$\Rightarrow \frac{1-d}{4} + P = \frac{1-\sqrt{d}}{2}\frac{1+\sqrt{d}}{2} + P = a(1-a) + P \xrightarrow{\text{Lemma 118 (i)}} \frac{1-d}{4} \equiv a(1-a) \equiv 0 \pmod 2$

$\Rightarrow d \equiv 1 \pmod 8$, a contradiction. Therefore (2) is a prime ideal.

Corollary 120 Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and p a prime. Then the

following are equivalent:

(i) p ramifies in K,

(ii) $p \mid d_K$.

Proof: Follows immediately from Theorems 70 and 119.

Remarks: 1) The first part of Theorem 119 can be stated in a concise way by using

the Kronecker symbol $(\frac{a}{p})$ (with $a \in \mathbb{Z}$ and p a prime). It is an extension of the

Legendre symbol and defined as follows:

If $p>2$ then set

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \mid a \end{cases}$$

and

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8, \\ -1 & \text{if } a \equiv 5 \pmod 8, \\ 0 & \text{if } a \equiv 0 \pmod 4 \end{cases}$$

Then p splits $\Leftrightarrow \left(\frac{d_K}{p}\right)=1$, p is inert $\Leftrightarrow \left(\frac{d_K}{p}\right)=-1$ and p ramifies $\Leftrightarrow \left(\frac{d_K}{p}\right)=0$.

(Note that $d \equiv 2,3 \pmod 4 \Rightarrow d_K = 4d \equiv 0 \pmod 4$ and

$d \equiv 1 \pmod 4 \Rightarrow d_K = d \equiv 1,5 \pmod 8$.)

18.1.2023

2) Corollary 120 is a special case of the following theorem by Dedekind: Let K be an algebraic number field, p a prime and $(p) = p\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$ (with pairwise different prime ideals $P_1, \dots, P_g$ and $e_1, \dots, e_g \in \mathbb{N}$). Then the following are equivalent:

(i) p ramifies in K (i.e., $\exists i \in \{1, \dots, g\} : e_i > 1$),

(ii) $p \mid d_K$.

This implies that only finitely many primes p ramify in K.

Theorem 121 Let D be a Dedekind domain. Then the following are equivalent:

(i) D is a unique factorization domain,

(ii) D is a principal ideal domain.

Proof: (i) $\Rightarrow$ (ii) Both (0) and $D=(1)$ are principal ideals. Let $P \neq (0)$ be a prime ideal of D. Choose $\alpha \in P \setminus \{0\}$. Then $P \mid (\alpha)$. As $\alpha \neq 0$ and $\alpha \notin D^*$ there is a factorization $\alpha = \pi_1 \dots \pi_k$ where $\pi_1, \dots, \pi_k \in D$ are irreducible. Then $(\alpha) = (\pi_1) \dots (\pi_k)$ and as P is a prime ideal, there is an $i \in \{1, \dots, k\}$: $P \mid (\pi_i)$. As D is a unique factorization domain, π_i is a prime element of D and (π_i) $(\neq (0))$ a prime ideal. Therefore $P = (\pi_i)$ is a principal ideal. Let I (with $I \neq (0)$ and $I \neq D$) be an ideal of D with factorization $I = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ into prime ideal. Then $\forall i \in \{1, \dots, k\}\ \exists \tau_i \in D : P_i = (\tau_i)$ and therefore

$I = P_1^{\alpha_1} \dots P_k^{\alpha_k} = (\tau_1)^{\alpha_1} \dots (\tau_k)^{\alpha_k} = (\tau_1^{\alpha_1} \dots \tau_k^{\alpha_k})$ is a principal ideal.

(ii) $\Rightarrow$ (i) Holds in general.