Dedekind Domains and Unique Factorization of Ideals

Recall that if K is a number field, then $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, and therefore $\mathcal{O}_K$ is noetherian.

Def If R is an integral domain, its **field of fractions** is given by

$$\mathrm{Frac}(R)=\left\{\frac{a}{b} \mid a,b\in R, b\neq 0\right\}/\sim \qquad \frac{a}{b}=\frac{c}{d} \text{ iff } ad=bc$$

Ex If $R=\mathbb{Z}$, $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$

$\mathrm{Frac}\left(\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]\right)=\mathbb{Q}(\sqrt{5})$ More generally, $\mathrm{Frac}(\mathcal{O}_K)=K$, since $\mathbb{Q}\mathcal{O}_K=K$

Def An integral domain R is **integrally closed** (in its field of fractions) if whenever $\alpha\in\mathrm{Frac}(R)$ and α satisfies a monic polynomial $f\in R[x]$, then $\alpha\in R$.

Ex $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is integrally closed in its field of fractions $\mathbb{Q}(\sqrt{5})$ but $\mathbb{Z}[\sqrt{5}]$ is not.

Prop Let K be a number field. Then $\mathcal{O}_K$ is integrally closed. The ring $\overline{\mathbb{Z}}$ of algebraic integers is integrally closed.

Proof: Suppose that $\alpha\in\mathbb{Q}$ is integral over $\mathbb{Z}$. There is $f(x)\in\mathbb{Z}[x]$. $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $f(\alpha)=0$. The a_i lie in $\mathcal{O}_K$ for some number field $K=\mathbb{Q}(a_0,\dots,a_{n-1})$. Since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, it is noetherian, and $\mathbb{Z}[a_0,\dots,a_{n-1}]$ is a finitely generated $\mathbb{Z}$-module. Since $f(\alpha)=0$, $\alpha^n=-(a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)$ and $\mathbb{Z}[a_0,\dots,a_{n-1},\alpha]$ is also a finitely generated $\mathbb{Z}$-module and noetherian $\Rightarrow$ $\mathbb{Z}[\alpha]$ finitely generated $\mathbb{Z}$-module $\Rightarrow$ α integral over $\mathbb{Z}$.

For $\mathcal{O}_K$, we have $\mathcal{O}_K=\overline{\mathbb{Z}}\cap K$, $\alpha\in K$ integral over $\mathcal{O}_K$, then α is integral over $\overline{\mathbb{Z}}\Rightarrow\alpha\in\overline{\mathbb{Z}}\cap K=\mathcal{O}_K$

Def An integral domain R is a **Dedekind domain** if

1. It is noetherian
2. Every nonzero prime ideal of R is maximal
3. R is integrally closed.

Ex $\mathbb{Z}\oplus\mathbb{Z}$ is not a Dedekind domain (not an integral domain)

$\mathbb{Z}[\sqrt{5}]$ is not a Dedekind domain (not integrally closed)

$\mathbb{Z}$ is a Dedekind domain.

Prop Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.

Proof We saw that $\mathcal{O}_K$ is noetherian and integrally closed. Suppose that

$\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. We will look at $\mathcal{O}_K/\mathfrak{p}$ and prove that it is a field. Let $\alpha \in \mathfrak{p}$, $\alpha \neq 0$, and $m_\alpha(x)$ its minimal polynomial.

$m_\alpha(\alpha)=\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_1\alpha+a_0=0 \Rightarrow a_0=-(\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_1\alpha) \in \mathfrak{p}$

Then $\forall \beta \in \mathcal{O}_K/\mathfrak{p}$, we have $a_0\beta=\overline{0}$. Since $a_0 \in \mathbb{Z}$, $\mathcal{O}_K/\mathfrak{p}$ is a finite set. Also $\mathcal{O}_K/\mathfrak{p}$ is an integral domain (since $\mathfrak{p}$ prime). Then it is a field $\Rightarrow$ $\mathfrak{p}$ maximal $\#$

If $\mathfrak{a}, \mathfrak{b}$ ideals in a ring R, then

$$\mathfrak{ab}=\langle ab \mid a\in\mathfrak{a}, b\in\mathfrak{b}\rangle$$ is an ideal of R.

Def Let R be a Dedekind domain and let $K=\text{Frac}(R)$. A **fractional ideal** is a nonzero finitely generated R-submodule $\mathfrak{a}$ of K.

Sometimes the ideals $\mathfrak{a} \subseteq R$ are called **integral ideals**.

Ex Let $k=\mathbb{Q}(i)$, $\mathcal{O}_K=\mathbb{Z}[i]$. Then $\mathfrak{a}=\frac{1}{2}\mathbb{Z}[i]$ is a fractional ideal.

$\mathfrak{a}=\frac{\mathbb{Z}}{2}+i\mathbb{Z}$ is not a fractional ideal. $\frac{i}{2}\in\mathfrak{a}$ but $\frac{i}{2}\cdot\frac{i}{2}=-\frac{1}{4}\notin\mathfrak{a}$.

In general $\exists \alpha \in K$ such that $\alpha\mathfrak{a}=\mathfrak{b}\subseteq R$ ($\mathfrak{b}$ integral ideal). This is because $\mathfrak{a}$ is finitely generated. Then, every fractional ideal $\mathfrak{a}$ can be written as $\beta\mathfrak{b}=\{\beta b \mid b\in\mathfrak{b}\}$, $\beta\in K$, $\mathfrak{b}\subseteq R$ integral ideal.

Thm: The set of fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication with identity element R.

Def: Let R be a Dedekind domain, $\mathfrak{a},\mathfrak{b}\subseteq R$ integral ideals. Then we say that $\mathfrak{a}$ **divides** $\mathfrak{b}$ if $\mathfrak{b}\subseteq\mathfrak{a}$.

Ex Take $K=\mathbb{Q}$; $\mathcal{O}_K=\mathbb{Z}$, $\mathfrak{a}=(a)$, $\mathfrak{b}=(b)$. Then $\mathfrak{a}\mid\mathfrak{b} \Rightarrow \mathfrak{b}\subseteq\mathfrak{a}$ $\Leftrightarrow (b)\subseteq(a) \Leftrightarrow a\mid b$.

Lemma Let R be an integral domain, $\mathfrak{a},\mathfrak{b}\subseteq R$ ideals, $\mathfrak{p}\subseteq R$ prime ideal. If $\mathfrak{ab}\subseteq\mathfrak{p}$, then $\mathfrak{a}\subseteq\mathfrak{p}$ or $\mathfrak{b}\subseteq\mathfrak{p}$.

Proof Suppose not, then $\exists a\in\mathfrak{a}\setminus\mathfrak{p}$, $b\in\mathfrak{b}\setminus\mathfrak{p}$, and $ab\in\mathfrak{ab}\subseteq\mathfrak{p}$ contradiction $\#$

Lemma Let R be a Dedekind domain, $\mathfrak{a}\subseteq R$ nonzero integral ideal. Then are $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ prime ideals such that $\mathfrak{p}_1\cdots\mathfrak{p}_n\subseteq\mathfrak{a}$ (i.e., $\mathfrak{a}\mid\mathfrak{p}_1\cdots\mathfrak{p}_n$).

Proof Let $S=\{\mathfrak{a}\subseteq R \text{ integral ideal} \mid \mathfrak{a}\neq\mathfrak{p}_1\cdots\mathfrak{p}_n\}$. We want to prove that $S=\emptyset$. Suppose that $S\neq\emptyset$, $\exists\mathfrak{a}\in S$ such that it is a maximal element of S. Clearly $\mathfrak{a}$ is not a prime ideal. Then $\exists a,b\in R$; $ab\in\mathfrak{a}$ but $a,b\notin\mathfrak{a}$. Let $\mathfrak{b}_1=\mathfrak{a}+(a)$, $\mathfrak{b}_2=\mathfrak{a}+(b)$. Then $\mathfrak{a}\subsetneq\mathfrak{b}_i$, $\mathfrak{b}_i\notin S$

THEREFORE, $b_1 \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $b_2 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$ AND $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq b_1 b_2 = \mathfrak{a}^2 + \mathfrak{a}(b) + (a)\mathfrak{a} + (ab) \subseteq \mathfrak{a}$ CONTRADICTION $\Rightarrow S = \emptyset$ #

EX IN $\mathbb{Z}[\sqrt{-5}]$, $(2) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$ $(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$

LEMMA LET R BE A DEDEKIND DOMAIN AND LET $\mathfrak{a}$ BE A PROPER NONZERO INTEGRAL IDEAL. $\exists\, \gamma \in K \setminus R$ SUCH THAT $\gamma \mathfrak{a} \subseteq R$

PROOF FIX $b \in \mathfrak{a}$, $b \neq 0$. BY THE PREVIOUS LEMMA, $(b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. CHOOSE THE PRODUCT SUCH THAT r IS MINIMIZED. SINCE EVERY IDEAL IS CONTAINED IN A MAXIMAL IDEAL, THERE IS $\mathfrak{P}$ SUCH THAT $\mathfrak{a} \subseteq \mathfrak{P}$. THUS $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{P}$. IT FOLLOWS THAT $\exists\, i$ SUCH THAT $\mathfrak{p}_i \subseteq \mathfrak{P}$. ASSUME WITHOUT LOSS OF GENERALITY THAT $\mathfrak{p}_1 \subseteq \mathfrak{P}$. BECAUSE PRIME IDEALS ARE MAXIMAL, $\mathfrak{p}_1 = \mathfrak{P}$. SINCE r IS MINIMAL, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (b)$ AND $\exists\, a \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (b)$. THEN $\gamma = \frac{a}{b} \in K \setminus R$. WE HAVE $\frac{a}{b}\mathfrak{a} \subseteq \left(\frac{1}{b}\right)\mathfrak{p}_2 \cdots \mathfrak{p}_r \mathfrak{a} \subseteq \left(\frac{1}{b}\right)\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \left(\frac{1}{b}\right)(b) = R$ #

PROP LET R BE A DEDEKIND DOMAIN AND LET $\mathfrak{a}$ BE A NONZERO INTEGRAL IDEAL OF R. THEN $\exists\, b$ INTEGRAL IDEAL SUCH THAT $\mathfrak{a}b$ IS PRINCIPAL. (IN OTHER WORDS, $\mathfrak{a}b = (a)$, AND WE MAY DENOTE $\mathfrak{a}^{-1} = a^{-1}b$)

PROOF: LET $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, AND SET $b = \{\beta \in R \mid \beta\mathfrak{a} \subseteq (\alpha)\}$

THEN $a \subseteq b$. IF $\beta_1, \beta_2 \in b$, $(\beta_1 + \beta_2)\mathfrak{a} = \beta_1\mathfrak{a} + \beta_2\mathfrak{a} \subseteq (\alpha) + (\alpha) = (\alpha)$

IF $s \in R$, $\beta \in b$, $s\beta\mathfrak{a} \subseteq (s\alpha) \subseteq (\alpha) \Rightarrow b$ IDEAL.

THEREFORE, $\mathfrak{a}b \subseteq (\alpha)$ AND WE NEED EQUALITY. SUPPOSE $\mathfrak{a}b \neq (\alpha)$

LET $A = \frac{\mathfrak{a}b}{\alpha} \subset R$. THEN A IS AN IDEAL. IF $A = R$, THEN $\mathfrak{a}b = (\alpha)$.

OTHERWISE, A IS PROPER. $\exists\, \gamma \in K \setminus R$ SUCH THAT $\gamma A \subseteq R$. NOTICE THAT $A = \frac{\mathfrak{a}b}{\alpha} \supseteq b$ SINCE $\alpha \in \mathfrak{a}$. THUS $\gamma b \subseteq \gamma A \subseteq R$ AND $\gamma\frac{\mathfrak{a}b}{\alpha} \subseteq R$

$\Rightarrow \gamma\mathfrak{a}b \subseteq (\alpha)$ SINCE $b = \{\beta \in R \mid \beta\mathfrak{a} \subseteq (\alpha)\}$, WE GET $\gamma b \subseteq b$

NOW FIX $\alpha_1, \ldots, \alpha_\ell$ A GENERATING SET FOR b. WE USE $\gamma b \subseteq b$ AND GET

$$M\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_\ell\end{pmatrix} = \begin{pmatrix}\gamma\alpha_1\\ \vdots \\ \gamma\alpha_\ell\end{pmatrix},$$

WHERE $M \in R^{\ell \times \ell}$ AND γ IS AN EIGENVALUE.

BY TAKING THE CHARACTERISTIC POLYNOMIAL, γ IS A ROOT OF A MONIC POLYNOMIAL WITH COEFFICIENTS IN M, AND SINCE $\gamma \in K$, AND R IS INTEGRALLY CLOSED WE GET $\gamma \in R$, A CONTRADICTION. #

PROOF OF THM THE PRODUCT OF TWO FRACTIONAL IDEALS IS FINITELY GENERATED AND THEREFORE, A FRACTIONAL IDEAL.

SINCE $\mathfrak{a}R = \mathfrak{a}$, WE HAVE THAT R IS THE IDENTITY. WE HAVE JUST SEEN THAT INTEGRAL IDEALS HAVE INVERSES GIVEN BY $\mathfrak{a}^{-1} = a^{-1}b$. FOR A FRACTIONAL

IDEAL $\mathfrak{a}$, TAKE $\alpha \in R$ SUCH THAT $\alpha\mathfrak{a}$ IS AN INTEGRAL IDEAL. THUS $\mathfrak{a}^{-1} = \alpha(\alpha\mathfrak{a})^{-1}$ #

ALGEBRAIC NUMBER THEORY

LET G BE THE GROUP OF FRACTIONAL IDEALS AND DEFINE AN EQUIVALENCE RELATION $\mathfrak{a} \sim \mathfrak{b}$ IFF $\exists \alpha \in K$ SUCH THAT $\mathfrak{b} = \alpha\mathfrak{a}$

DEF THE GROUP $G/\sim$ IS CALLED THE IDEAL CLASS GROUP. IT IS DENOTED BY C_K OR $Cl(K)$

$x^n + y^n = z^n$

M. LALÍN

COR: LET R BE A DEDEKIND DOMAIN AND LET $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ BE FRACTIONAL IDEALS. THEN $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} \Rightarrow \mathfrak{b} = \mathfrak{c}$

PROOF: MULTIPLY BY $\mathfrak{a}^{-1}$ IN BOTH SIDES #

COR: LET $\mathfrak{a}, \mathfrak{b}$ BE INTEGRAL IDEALS. THEN $\mathfrak{a} \mid \mathfrak{b}$ (OR $\mathfrak{b} \subseteq \mathfrak{a}$) IFF $\exists \mathfrak{c}$ INTEGRAL IDEAL SUCH THAT $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$

PROOF: $\Rightarrow$) ASSUME $\mathfrak{b} \subseteq \mathfrak{a}$, THEN $\exists \mathfrak{d}$ SUCH THAT $\mathfrak{a}\mathfrak{d} = (\alpha)$. TAKE $\mathfrak{c} = \frac{1}{\alpha}\mathfrak{d}\mathfrak{b}$. THEN $\mathfrak{a}\mathfrak{c} = \mathfrak{a}\frac{1}{\alpha}\mathfrak{d}\mathfrak{b} = \mathfrak{b}$

$\Leftarrow$) $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a} \Rightarrow \mathfrak{b} \subseteq \mathfrak{a}$ #.

THM EVERY INTEGRAL IDEAL IN A DEDEKIND DOMAIN R IS UNIQUELY REPRESENTABLE AS THE PRODUCT OF PRIME IDEALS.

PROOF: LET $S = \{\mathfrak{a} \subsetneq R$ INTEGRAL IDEAL $\mid \mathfrak{a}$ IS NOT A PRODUCT OF PRIMES$\}$ (SINCE R NOETHERIAN)

WE WANT TO SEE $S = \emptyset$. IF NOT, LET $\mathfrak{a} \in S$ MAXIMAL. THEN $\mathfrak{a} \subseteq \mathfrak{p}$ FOR SOME $\mathfrak{p}$ IF $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, THEN WE GET $\mathfrak{p}^{-1} = R$, A CONTRADICTION SINCE $\mathfrak{p} \neq R$. THUS $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \Rightarrow \mathfrak{a}\mathfrak{p}^{-1} \notin S$ AND $\exists \mathfrak{p}_1, \dots, \mathfrak{p}_n$ SUCH THAT $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \Rightarrow \mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n$ CONTRADICTION $\Rightarrow S = \emptyset$.

NOW SUPPOSE $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. THIS IMPLIES $\mathfrak{q}_1 \mid \mathfrak{p}_1 \cdots \mathfrak{p}_n$ AND THEREFORE, THERE IS i SUCH THAT $\mathfrak{q}_1 \mid \mathfrak{p}_i$. SAY $\mathfrak{q}_1 \mid \mathfrak{p}_1$. THEN $\mathfrak{q}_1 = \mathfrak{p}_1$

WE CANCEL IN BOTH SIDES AND CONTINUE. #

THM IF $\mathfrak{a}$ IS A FRACTIONAL IDEAL OF R, THEN $\exists \mathfrak{p}_1, \dots, \mathfrak{p}_n, \mathfrak{q}_1, \dots, \mathfrak{q}_m$ SUCH THAT $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n (\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}$

PROOF LET $\alpha \in R$, $\alpha\mathfrak{a}$ INTEGRAL, $\alpha\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ TAKE $(\alpha) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ #

EX IF $K = \mathbb{Q}(\sqrt{-6})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, THEN $6 = \sqrt{-6}(-\sqrt{-6}) = 2 \cdot 3$

$N_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(2) = 4$, $N_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(3) = 9$, $N_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(\sqrt{-6}) = 6$

$N_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a + b\sqrt{-6}) = a^2 + 6b^2 \neq 2, 3 \Rightarrow \sqrt{-6}, 2, 3$ IRREDUCIBLE.

$(2, 2+\sqrt{-6})(3, 3+\sqrt{-6}) = (6, 6+3\sqrt{-6}, 6+2\sqrt{-6}, 5+\sqrt{-6}) = (\sqrt{-6})$

$\subseteq$ CLEAR, $\supseteq$ $\sqrt{-6} = (6+3\sqrt{-6}) - (6+2\sqrt{-6})$

$(2, 2+\sqrt{-6})^2 = (4, 4+2\sqrt{-6}, -2+4\sqrt{-6}) = (2)$

$\subseteq$ CLEAR $\supseteq$ $2 = 2(4+2\sqrt{-6}) - (-2+4\sqrt{-6}) - 2\cdot 4$.

ALGEBRAIC SIMILARLY, $(3, 3+3\sqrt{-6})^2 = (3)$

NUMBER THEORY

$x^n + y^n = z^n$

M. LALÍN

DEF LET R BE A DEDEKIND DOMAIN. LET $\mathfrak{a}, \mathfrak{b}$ BE INTEGRAL IDEALS WITH FACTORIZATION $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$ $\mathfrak{b} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ $m_i \geq 0$, $n_i \geq 0$.

THE GREATEST COMMON DIVISOR IS GIVEN BY $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{\min(m_1, n_1)} \cdots \mathfrak{p}_r^{\min(m_r, n_r)}$.

THE LEAST COMMON MULTIPLE IS GIVEN BY $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{p}_1^{\max(m_1, n_1)} \cdots \mathfrak{p}_r^{\max(m_r, n_r)}$

$(\mathfrak{a}, \mathfrak{b})$ IS THE SMALLEST IDEAL CONTAINING BOTH $\mathfrak{a}$ AND $\mathfrak{b}$.

$[\mathfrak{a}, \mathfrak{b}]$ IS THE LARGEST IDEAL CONTAINED IN BOTH $\mathfrak{a}$ AND $\mathfrak{b}$

THEN $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$, $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a} \cap \mathfrak{b}$

$\mathfrak{a}$ AND $\mathfrak{b}$ ARE SAID TO BE COPRIME IF $\mathfrak{a} + \mathfrak{b} = (1) = R$.

LEMMA IF $\mathfrak{a}, \mathfrak{b}$ ARE COPRIME, THEN $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

PROOF LET $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ SUCH THAT $a + b = 1$. IF $c \in \mathfrak{a} \cap \mathfrak{b}$, THEN $c = ca + cb \in \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$. THE OTHER INCLUSION COMES FROM $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$. #

THM (CHINESE REMAINDER THEOREM) LET $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ BE NONZERO IDEALS IN A DEDEKIND DOMAIN R SUCH THAT $(\mathfrak{a}_m, \mathfrak{a}_n) = R$ $\forall m \neq n$. THEN

$$R / \bigcap_{i=1}^{s} \mathfrak{a}_i \simeq R/\mathfrak{a}_1 \oplus R/\mathfrak{a}_2 \oplus \cdots \oplus R/\mathfrak{a}_s$$

$$= \prod_{i=1}^{s} \mathfrak{a}_i$$

THUS, GIVEN $a_i \in R$ $i = 1, \ldots, s$, $\exists a \in R$ SUCH THAT $a \equiv a_n \pmod{\mathfrak{a}_n}$ AND a IS UNIQUE MODULO $\bigcap_{i=1}^{s} \mathfrak{a}_i$.

PROOF: LET $\varphi : R \longrightarrow R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_s$ BE THE NATURAL MAP INDUCED BY REDUCTION MODULO $\mathfrak{a}_n$.

THE KERNEL IS GIVEN BY $\bigcap_{i=1}^{s} \mathfrak{a}_i$, THEN THE QUOTIENT MAP IS INJECTIVE

EACH PROJECTION $R \longrightarrow R/\mathfrak{a}_i$ IS SURJECTIVE. TO PROVE THAT φ IS SURJECTIVE WE NEED TO PROVE THAT $(0, \ldots, 0, \overset{n}{1}, 0, \ldots, 0)$ IS IN $\operatorname{Im}\varphi$.

SINCE $\mathfrak{b} = \prod_{i \neq n} \mathfrak{a}_i$ IS COPRIME TO $\mathfrak{a}_n$, $\exists a \in \mathfrak{a}_n$, $b \in \mathfrak{b}$ SUCH THAT $a + b = 1$ THEN b MAPS TO $1 \in R/\mathfrak{a}_n$ AND TO 0 IN $R/\mathfrak{b}$, HENCE TO 0 IN $R/\mathfrak{a}_i$ FOR $i \neq n$, SINCE $\mathfrak{b} \subseteq \mathfrak{a}_i$ #

THM LET $\mathfrak{a}$ BE AN INTEGRAL IDEAL IN A DEDEKIND DOMAIN R AND LET $a \in \mathfrak{a}$, $a \neq 0$. THEN THERE EXISTS $b \in \mathfrak{a}$ SUCH THAT $\mathfrak{a} = (a, b)$

PROOF: WE NEED TO FIND b SUCH THAT $\mathfrak{a} = ((a), (b))$

Let $a=\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r}$. Then (a) is divisible by all $\mathfrak{p}_i^{n_i}$. Let $\mathfrak{q}_1,\dots,\mathfrak{q}_s$ be the other primes that divide (a). We need a b such that no $\mathfrak{q}_i$ divides (b) and such that $\mathfrak{p}_i^{n_i}$ is the exact power of $\mathfrak{p}_i$ dividing (b). We need

$$b\in\bigcap_{i=1}^{r}\left(\mathfrak{p}_i^{n_i}-\mathfrak{p}_i^{n_i+1}\right)\cap\bigcap_{j=1}^{s}\left(R-\mathfrak{q}_j\right)$$

Fix $\beta_i\in\mathfrak{p}_i^{n_i}-\mathfrak{p}_i^{n_i+1}$ $(i\in)$ (non-empty by unique factorization). By the Chinese Remainder Theorem, there is a b such that

$$b\equiv\beta_i\pmod{\mathfrak{p}_i^{n_i+1}}\ i=1,\dots,r \text{ and } b\equiv 1\pmod{\mathfrak{q}_j}\ j=1,\dots,s\ \#$$

Prop Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain R. Let $n\in\mathbb{Z}_{\geq 0}$. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1}\simeq R/\mathfrak{p}$ as R-modules.

Proof: Since $\mathfrak{p}^n\neq\mathfrak{p}^{n+1}\Rightarrow\exists b\in\mathfrak{p}^n-\mathfrak{p}^{n+1}$. Let $\varphi: R\to\mathfrak{p}^n/\mathfrak{p}^{n+1}$ given by $\varphi(a)=ab$. Clearly $\ker\varphi=\mathfrak{p}$, since $\varphi(\mathfrak{p})=0$ and $\varphi(a)=0\Rightarrow ab\in\mathfrak{p}^{n+1}$ and $\mathfrak{p}^{n+1}\mid(ab)\Rightarrow\mathfrak{p}\mid(a)$. Thus φ induces an injective homomorphism $R/\mathfrak{p}\hookrightarrow\mathfrak{p}^n/\mathfrak{p}^{n+1}$. Now let us prove surjective. Suppose $c\in\mathfrak{p}^n$. By the Chinese Remainder Theorem, $\exists d\in R$ such that $d\equiv c\pmod{\mathfrak{p}^{n+1}}$, $d\equiv 0\pmod{(b)/\mathfrak{p}^n}$. We have $\mathfrak{p}^n\mid(d)$ since $d\in\mathfrak{p}^n$ (since $c\in\mathfrak{p}^n$) and $(b)/\mathfrak{p}^n\mid(d)$. Since $\mathfrak{p}\nmid(b)/\mathfrak{p}^n$, we have $(b)=\mathfrak{p}^n(b)/\mathfrak{p}^n\mid(d)$ $\Rightarrow d/b\in R$. $\varphi(d/b)=\frac{d}{b}b\pmod{\mathfrak{p}^{n+1}}\equiv d\equiv c\pmod{\mathfrak{p}^{n+1}}$ and φ is surjective $\#$

Thm A Dedekind domain is a UFD iff it is a PID.

Proof: We know that PID$\Rightarrow$UFD in general. Now assume that a Dedekind domain R is a UFD. Let $\mathfrak{a}$ be an ideal in R. Then there is $a\in R$ such that $\mathfrak{a}\mid(a)$. By factoring a into primes in R, $a=p_1^{n_1}\cdots p_r^{n_r}\Rightarrow\mathfrak{a}\mid(p_1)^{n_1}\cdots(p_r)^{n_r}$ and each (p_i) is a prime ideal. By unique factorization into prime ideals, it follows that $\mathfrak{a}=(p_1)^{m_1}\cdots(p_r)^{m_r}$ with $0\leq m_i\leq n_i$. And $\mathfrak{a}=(p_1^{m_1}\cdots p_r^{m_r})$ $\#$

Factoring Primes in Extensions

Consider $5\in\mathbb{Z}$, it is a prime. However, $5=(1+2i)(1-2i)$ in $\mathbb{Z}[i]$, 5 is not longer a prime in $\mathbb{Z}[i]$. On the other hand, 3 is a prime both in $\mathbb{Z}$ and in $\mathbb{Z}[i]$. Finally, $2=(1+i)(1-i)=-i(1+i)^2$

We also saw, in $\mathbb{Z}[\sqrt{-5}]$, $(2)=(2,1+\sqrt{-5})^2$ $(3)=(3,1+\sqrt{-5})(3,1-\sqrt{-5})$

We say that 3 splits in $\mathbb{Z}[\sqrt{-5}]$ or 5 splits in $\mathbb{Z}[i]$

If we have an extension of number fields L/K, with $\mathfrak{P}$ a prime ideal of $\mathcal{O}_K$, the question is, what happens to the prime decomposition of $\mathfrak{P}\mathcal{O}_L$ in $\mathcal{O}_L$?

Thm Let $\mathfrak{P}$ be a nonzero prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ a nonzero prime ideal of $\mathcal{O}_L$. The following are equivalent:

① $\mathfrak{q}\mid\mathfrak{P}\mathcal{O}_L$ ② $\mathfrak{q}\supseteq\mathfrak{P}\mathcal{O}_L$ ③ $\mathfrak{q}\supseteq\mathfrak{P}$ ④ $\mathfrak{q}\cap\mathcal{O}_K=\mathfrak{P}$ ⑤ $\mathfrak{q}\cap K=\mathfrak{P}$

Proof ①⟺② by definition

②⟺③ trivial, since $\mathfrak{q}\subseteq\mathcal{O}_L$, thus $\mathfrak{q}\mathcal{O}_L=\mathfrak{q}$

④⇒③ trivial. ④⟺⑤ trivial since $\mathfrak{q}\subseteq\mathbb{Z}$

We need ③⇒④ $\mathfrak{q}\cap\mathcal{O}_K\supseteq\mathfrak{P}$ clearly and $\mathfrak{q}\cap\mathcal{O}_K$ is an ideal in $\mathcal{O}_K$ since $\mathfrak{P}$ is maximal, $\mathfrak{q}\cap\mathcal{O}_K=\mathfrak{P}$ or $\mathfrak{q}\cap\mathcal{O}_K=\mathcal{O}_K$. If $\mathfrak{q}\cap\mathcal{O}_K=\mathcal{O}_K$, we get $1\in\mathfrak{q}$ and $\mathfrak{q}=\mathcal{O}_L$, a contradiction #

Def In the case above, we say that $\mathfrak{q}$ lies over $\mathfrak{P}$ or $\mathfrak{P}$ lies under $\mathfrak{q}$

Thm Every nonzero prime $\mathfrak{q}$ of $\mathcal{O}_L$ lies over a unique nonzero prime $\mathfrak{P}$ of $\mathcal{O}_K$. Every nonzero prime $\mathfrak{P}$ of $\mathcal{O}_K$ lies under at least one nonzero prime $\mathfrak{q}$ of $\mathcal{O}_L$

Proof First we show that $\mathfrak{q}\cap\mathcal{O}_K$ is a nonzero prime ideal of $\mathcal{O}_K$: Since $1\notin\mathfrak{q}$, it is proper. If $a,b\in\mathcal{O}_K$ and $ab\in\mathfrak{q}\cap\mathcal{O}_K$, then $ab\in\mathfrak{q}$ $\Rightarrow a\in\mathfrak{q}$ or $b\in\mathfrak{q}$ (say $a\in\mathfrak{q}$) $\Rightarrow a\in\mathfrak{q}\cap\mathcal{O}_K\Rightarrow\mathfrak{q}\cap\mathcal{O}_K$ is prime. To prove nonzero, take $\alpha\in\mathfrak{q}$ $\alpha\neq0$ then $N_{L/K}(\alpha)\in\mathfrak{q}\cap\mathcal{O}_K$ and $N_{L/K}(\alpha)\neq0$.

We need to show that $\mathfrak{P}\mathcal{O}_L\neq\mathcal{O}_L$ so that there is at least one prime divisor. $\exists\gamma\in K\setminus\mathcal{O}_K$ such that $\gamma\mathfrak{P}\subseteq\mathcal{O}_K$. Then $\gamma\mathfrak{P}\mathcal{O}_L\subseteq\mathcal{O}_L$ If $\mathfrak{P}\mathcal{O}_L=\mathcal{O}_L$, then $1\in\mathfrak{P}\mathcal{O}_L\Rightarrow\gamma\in\mathcal{O}_L\Rightarrow\gamma\in\mathbb{Z}$ contradiction #

Def The exponents of the primes lying over $\mathfrak{P}$ are called ramification indexes. If $\mathfrak{q}^e\mid\mathfrak{P}\mathcal{O}_L$ and $\mathfrak{q}^{e+1}\nmid\mathfrak{P}\mathcal{O}_L$, we write $\mathfrak{q}^e\parallel\mathfrak{P}\mathcal{O}_L$ and $e=e(\mathfrak{q}/\mathfrak{P})$

Ex If $\mathcal{O}_L=\mathbb{Z}[i]$, $\mathcal{O}_K=\mathbb{Z}$, $(1+i)$ lies over (2)

$(1+i)$ is a prime ideal because $\mathbb{Z}[i]/(1+i)\cong\mathbb{Z}/2\mathbb{Z}$ (a field)

$(2)\mathcal{O}_L=(1+i)^2\Rightarrow e((1+i)\mid(2))=2$

If p is prime in $\mathbb{Z}$, $p\neq2$ $p\equiv1\pmod4$ then $p=a^2+b^2$

$(p)\mathcal{O}_L = (a+bi)(a-bi)$ $\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}/p\mathbb{Z}$. $e((a+bi)|(p)) = 1$.

IF p IS PRIME IN $\mathbb{Z}$ $p \equiv 3 \pmod 4$ IT REMAINS PRIME IN $\mathbb{Z}[i]$,

ALGEBRAIC NUMBER THEORY $x^n + y^n = z^n$ M. LATIN $e(p)\mathbb{Z}[i] | (p)) = 1$

WE KNOW THAT $\mathcal{O}_K/\mathfrak{P}$ AND $\mathcal{O}_L/\mathfrak{q}$ ARE FIELDS (RESIDUE FIELDS). WE HAVE A NATURAL MAP $\mathcal{O}_K \longrightarrow \mathcal{O}_L/\mathfrak{q}$ WHOSE KERNEL IS $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{P}$. THIS GIVES AN EMBEDDING $\mathcal{O}_K/\mathfrak{P} \hookrightarrow \mathcal{O}_L/\mathfrak{q}$

THEY ARE FINITE FIELDS, SO $\mathcal{O}_L/\mathfrak{q}$ IS A FINITE EXTENSION OF $\mathcal{O}_K/\mathfrak{P}$ OF DEGREE $f = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{P}]$ THIS IS CALLED THE **INERTIA DEGREE**.

EX CONSIDER $(1+i) = \mathfrak{q} \subseteq \mathbb{Z}[i]$, $(2) = \mathfrak{P} \subseteq \mathbb{Z}$.

$|\mathcal{O}_K/\mathfrak{P}| = 2$ $|\mathcal{O}_L/(1+i)| = 2 \Rightarrow f = 1$

SINCE $(3)\mathbb{Z}[i]$ IS PRIME, LOOK AT $|\mathbb{Z}[i]/(3)\mathbb{Z}[i]| = 9$

$|\mathbb{Z}/(3)| = 3 \Rightarrow f = 2$.

IF $\mathfrak{P} \subseteq \mathfrak{q} \subseteq \mathfrak{Q}$ ARE PRIMES IN THE NUMBER RINGS $\mathcal{O}_K \subseteq \mathcal{O}_L \subseteq \mathcal{O}_M$, THEN

$$e(\mathfrak{Q}|\mathfrak{P}) = e(\mathfrak{Q}/\mathfrak{q})\, e(\mathfrak{q}|\mathfrak{P})$$
$$f(\mathfrak{Q}|\mathfrak{P}) = f(\mathfrak{Q}/\mathfrak{q})\, f(\mathfrak{q}|\mathfrak{P})$$

} SEE HOMEWORK.

IN GENERAL, IF WE TAKE $K = \mathbb{Q}$ AND L A NUMBER FIELD WITH $\mathfrak{q} \subseteq \mathcal{O}_L$ PRIME, THEN $\mathfrak{q}$ LIES OVER A UNIQUE $p \in \mathbb{Z}$

THEN $|\mathcal{O}_L/\mathfrak{q}| = p^f$. ALSO, SINCE $p\mathcal{O}_L \subseteq \mathfrak{q}$, WE HAVE $p^f \leq |\mathcal{O}_L/p\mathcal{O}_L| = p^n$, WHERE $n = [L:\mathbb{Q}]$. THUS $f \leq n$.

THM (A) LET L/K BE AN EXTENSION OF NUMBER FIELDS; $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ PRIMES OF $\mathcal{O}_L$ LYING OVER A PRIME $\mathfrak{P}$ OF $\mathcal{O}_K$. LET $e_1, \dots, e_r, f_1, \dots, f_r$ BE THE RAMIFICATION INDEXES AND INERTIA DEGREES RESPECTIVELY. THEN

$$\sum_{i=1}^{r} f_i e_i = [L:K] = n.$$

THM (B) LET $\mathfrak{a} \subseteq \mathcal{O}_K$ IDEAL AND $N_K(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ THEN

(a) FOR $\mathfrak{a}, \mathfrak{b}$ IDEALS IN $\mathcal{O}_K$, $N_K(\mathfrak{a}\mathfrak{b}) = N_K(\mathfrak{a})N_K(\mathfrak{b})$

(b) FOR $\mathfrak{a}$ IDEAL IN $\mathcal{O}_K$, $N_L(\mathfrak{a}\mathcal{O}_L) = N_K(\mathfrak{a})^n$

(c) FOR $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. $N_K((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$

PROOF (B) (a) FIRST ASSUME $(\mathfrak{a}, \mathfrak{b}) = 1$, $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$. THEN $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ AND THE CHINESE REMAINDER THEOREM GIVES

$$\mathcal{O}_K/\mathfrak{a}\mathfrak{b} = \mathcal{O}_K/\mathfrak{a}\cap\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$$

$$\Rightarrow N_K(\mathfrak{a}\mathfrak{b}) = N_K(\mathfrak{a})\, N_K(\mathfrak{b})$$

NOW CONSIDER $N_K(\mathfrak{P}^e)$ FOR $\mathfrak{P}$ A PRIME IDEAL.

We proved that $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}_K/\mathfrak{p}$. Then $N_K(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathfrak{p}^i/\mathfrak{p}^{i+1}|$.

Consider $\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^\ell$

$N_K(\mathfrak{p})^\ell = |\mathcal{O}_K/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2|\dots|\mathfrak{p}^{\ell-1}/\mathfrak{p}^\ell| = |\mathcal{O}_K/\mathfrak{p}^\ell| = N_K(\mathfrak{p}^\ell)$

Combining the above, we get $N_K(\alpha\mathfrak{b}) = N_K(\alpha)N_K(\mathfrak{b})$ in general.

Ⓐ Special case $K=\mathbb{Q}$. Then $\mathfrak{p} = p\mathbb{Z}$, write $p\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$.

$N_L(p\mathcal{O}_L) = \prod_{i=1}^r N_L(\mathfrak{q}_i^{e_i}) = \prod_{i=1}^r (p^{f_i})^{e_i}$

On the other hand $N_L(p\mathcal{O}_L) = p^n$. By comparing both formulas, we get this case.

Before we continue with the proof, we need the following.

Lemma: Let $\alpha, \mathfrak{b}$ be nonzero integral ideals in a Dedekind domain R such that $\alpha \subseteq \mathfrak{b} \neq R$. Then there is $\gamma \in K$ such that $\gamma\alpha \subseteq R$ $\gamma\alpha \not\subseteq \mathfrak{b}$.

Proof We know that there is an integral ideal $\mathfrak{C}$ such that $\alpha\mathfrak{C} = (\alpha)$. In particular, $\alpha\mathfrak{C} \not\subseteq \alpha\mathfrak{b}$. Take $\beta \in \mathfrak{C}$ such that $\beta\alpha \not\subseteq \alpha\mathfrak{b}$ and take $\gamma = \frac{\beta}{\alpha}$. Then $\gamma\alpha = \frac{\beta}{\alpha}\mathcal{O}_L \subseteq \frac{\alpha\mathfrak{C}}{\alpha} \subseteq R$ ↯

Ⓑ Ⓑ By Ⓑ Ⓐ we can assume that $\mathfrak{p} = \mathfrak{p}$ prime. We know that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a vector space over $\mathcal{O}_K/\mathfrak{p}$ and we claim that it has dimension n. First we prove $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \leq n$.

Let $\alpha_1, \dots, \alpha_{n+1} \in \mathcal{O}_L$. They are linearly dependent over K. Thus, $\exists a_1, \dots, a_{n+1} \in \mathcal{O}_K$ not all zero such that $\sum_{i=1}^{n+1} a_i\alpha_i = 0$

Suppose that the a_i become zero in $\mathcal{O}_K/\mathfrak{p}$. This happens iff $(a_1, \dots, a_n) \subseteq \mathfrak{p}$.

By the Lemma, $\exists \gamma \in K \setminus \mathcal{O}_K$ such that $\gamma(a_1, \dots, a_{n+1}) \subseteq \mathcal{O}_K$ but $\gamma(a_1, \dots, a_n) \not\subseteq \mathfrak{p}$.

But then $\gamma a_1\alpha_1 + \dots + \gamma a_{n+1}\alpha_{n+1} = 0$ gives a nontrivial combination in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. This implies that $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \leq n$.

Now we prove that $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$.

Let $\mathfrak{p} \cap \mathbb{Z} = (p)$ and let $\mathfrak{p}_i$ be the primes lying over (p). Then $\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L$ is a vector space over $\mathcal{O}_K/\mathfrak{p}_i$ of dimension $n_i \leq n$.

Let $p\mathcal{O}_K = \prod \mathfrak{p}_i^{e_i}$, $p\mathcal{O}_L = \prod (\mathfrak{p}_i\mathcal{O}_L)^{e_i}$

Now $\sum e_i f_i = [K:\mathbb{Q}] = m$ by the special case of Ⓐ already proven and $p^{nm} = N_L(p\mathcal{O}_L) = \prod N_L(\mathfrak{p}_i\mathcal{O}_L)^{e_i} = \prod N_K(\mathfrak{p}_i)^{n_i e_i} = (\prod p^{f_i})^{n_i e_i}$

$\Rightarrow mn = \sum e_i f_i n_i$ by the special case of (A) already proven.
Since $n_i \le n$ and $\sum e_i f_i = m$, we have
$mn = \sum e_i f_i n_i \le \sum e_i f_i n = mn$ and we must have $n_i = n$

(A) Let $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$.
Then $N_L(\mathfrak{p}\mathcal{O}_L) = \prod N_L(\mathfrak{q}_i)^{e_i} = \prod N_K(\mathfrak{p})^{f_i e_i}$ by (B) (c) (b) and the definition of f_i.
By (B) (b) $N_L(\mathfrak{p}\mathcal{O}_L) = N_K(\mathfrak{p})^n$
Thus we get $n = \sum e_i f_i$

(B) (c) First extend K to a Galois extension (its Galois closure) M. For each embedding $\sigma: K \hookrightarrow \overline{\mathbb{Q}}$ take an extension $\tilde{\sigma}: M \to M$
We have $N_M(\tilde{\sigma}(\alpha)\mathcal{O}_M) = N_M(\alpha\mathcal{O}_M)$ because $\tilde{\sigma}(\mathcal{O}_M) = \mathcal{O}_M$ and $\mathcal{O}_M/\alpha\mathcal{O}_M \simeq \tilde{\sigma}(\mathcal{O}_M/\alpha\mathcal{O}_M)$
Now $N_M(N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_M) = \prod_{\sigma} N_M(\tilde{\sigma}(\alpha)\mathcal{O}_M) = N_K(\alpha\mathcal{O}_M)^n$, where $n = [K:\mathbb{Q}]$
By (B) (b), we have $N_M(N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_M) = |N_{K/\mathbb{Q}}(\alpha)|^{mn}$, where $m = [M:K]$
And by (B) (b) we have $N_M((\alpha)\mathcal{O}_M) = N_K((\alpha))^m$
Thus, $N_K((\alpha))^{mn} = N_M((\alpha)\mathcal{O}_M)^n = N_M(N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_M) = |N_{K/\mathbb{Q}}(\alpha)|^{mn}$
$\Rightarrow N_K((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$ #

Ex Take $K = \mathbb{Q}(\sqrt[3]{2})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.
Since $(2) = (\sqrt[3]{2})^3$, then $N_K((\sqrt[3]{2})) = 2$ and $(\sqrt[3]{2})$ is prime.
Then $e=3$, $f=1$. Also $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$ since $\min_{\sqrt[3]{2}}(x) = x^3-2$

Ex Let α be a root of $x^3 = x+1$, $K = \mathbb{Q}(\alpha)$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$
$\operatorname{disc}(\alpha) = -(4(-1)^3+27) = -23$
$(23) = (23, \alpha-10)^2(23, \alpha-3)$ (homework)
The factors do not have all the same ramification index.

Now assume that the extension L/K is Galois and let $\mathfrak{P}$ be a prime of $\mathcal{O}_K$. If $\mathfrak{q}$ lies over $\mathfrak{P}$, and $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma(\mathfrak{q})$ is an ideal of $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ lying over $\sigma(\mathfrak{P}) = \mathfrak{P}$.

Thm Let L/K be a Galois extension, $\mathfrak{q}, \mathfrak{q}'$ prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{P}$ prime ideal of $\mathcal{O}_K$. Then $\exists \sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$.

Proof Suppose $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ $\forall \sigma \in \mathrm{Gal}(L/K)$. By the Chinese Remainder Theorem, there is a number $a \in L$ such that $a \equiv 0 \pmod{\mathfrak{q}'}$ and $a \equiv 1 \pmod{\sigma(\mathfrak{q})}$ $\forall \sigma \in \mathrm{Gal}(L/K)$

$N_{L/K}(a) \in \mathcal{O}_K \cap \mathfrak{q}' = \mathfrak{p}$ AND $a \notin \prec(\mathfrak{q}) \Rightarrow \prec^{-1}(a) \notin \mathfrak{q}\ \forall \prec \Rightarrow N_{L/K}(a) \notin \mathfrak{q}$

BUT $\Rightarrow N_{L/K}(a) \notin \mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ CONTRADICTION #

COR LET L/K BE A GALOIS EXTENSION, $\mathfrak{q}, \mathfrak{q}'$ PRIME IDEALS OF $\mathcal{O}_L$ LYING OVER $\mathfrak{p}$. THEN $e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}'/\mathfrak{p})$; $f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}'/\mathfrak{p})$

PROOF: FROM UNIQUE FACTORIZATION, $e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}'/\mathfrak{p})$, SINCE THERE IS $\prec$ SUCH THAT $\prec(\mathfrak{q}) = \mathfrak{q}'$

ON THE OTHER HAND, $\mathcal{O}_L/\mathfrak{q} \longrightarrow \mathcal{O}_L/\mathfrak{q}'$ IS AN ISOMORPHISM.

$a \longrightarrow \prec(a) \Rightarrow f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}'/\mathfrak{p})$ #

THUS, $\mathfrak{p}\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^e$ $ref = [L:K]$

DEF LET $K \subset L$ BE NUMBER FIELDS, $\mathfrak{p} \subset \mathcal{O}_K$ PRIME. THEN $\mathfrak{p}$ IS RAMIFIED IN $\mathcal{O}_L$ IF $e(\mathfrak{q}/\mathfrak{p}) > 1$ FOR SOME $\mathfrak{q}$ LYING OVER $\mathfrak{p}$.

EX IN $\mathbb{Z}[\omega_p]$, WHERE p IS AN ODD PRIME, WE HAVE $p = (1-\omega_p)\cdots(1-\omega_p^{p-1})$

$(1-\omega_p^k)\mathbb{Z}[\omega_p] = (1-\omega_p)\mathbb{Z}[\omega_p]$ BECAUSE $\frac{1-\omega_p^k}{1-\omega_p}$ IS A UNIT

THEN, AT THE LEVEL OF IDEALS, $(1-\omega_p) = (1-\omega_p^k)$. THUS $p\mathbb{Z}[\omega_p] = (1-\omega_p)^{p-1}$

$(1-\omega_p)$ IS A PRIME IDEAL, $N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(1-\omega_p) = p$

p IS RAMIFIED IN $\mathbb{Z}[\omega_p]$ (NOTICE $disc = \pm p^{p-2}$)

23 IS RAMIFIED IN $\mathbb{Z}[\alpha]$ $\alpha^3 = \alpha + 1$ $(disc = -23)$

2 IS RAMIFIED IN $\mathbb{Z}[\sqrt[3]{2}]$ $(disc = -3^3 \cdot 2^2)$

3 IS RAMIFIED IN $\mathbb{Z}[\sqrt[3]{2}]$ $(3) = (\sqrt[3]{2}+1)^3$ $N(\sqrt[3]{2}+1) = 3$

THM: LET K BE A NUMBER FIELD AND p BE PRIME IN $\mathbb{Z}$ THAT RAMIFIES IN $\mathcal{O}_K$. THEN $p \mid disc(K)$ (IN FACT, IT IS IFF, WE WILL PROVE THIS LATER)

PROOF: LET $\mathfrak{p}$ BE A PRIME OF $\mathcal{O}_K$ LYING OVER p SUCH THAT $e(\mathfrak{p}/p) > 1$

THEN $p\mathcal{O}_K = \mathfrak{p}\mathcal{A}$ WITH $\mathcal{A}$ DIVISIBLE BY ALL PRIMES OF $\mathcal{O}_K$ LYING OVER p

LET $\sigma_1, \dots, \sigma_n$ THE EMBEDDINGS OF K ON $\overline{\mathbb{Q}}$ EXTENDED TO THE GALOIS CLOSURE L OF K. LET $\alpha_1, \dots, \alpha_n$ BE AN INTEGRAL BASIS OF $\mathcal{O}_K$. TAKE $\alpha \in \mathcal{A} \setminus p\mathcal{O}_K$. THEN $\alpha \in \mathfrak{p}'$ FOR ALL $\mathfrak{p}'$ PRIME IDEAL LYING OVER p, BUT $\alpha \notin p\mathcal{O}_K$. WRITE $\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n$. THEN $r_i \in \mathbb{Z}$ BUT $\exists i$ SUCH THAT $p \nmid r_i$ (SINCE $\alpha \notin p\mathcal{O}_K$). SAY, $p \nmid r_1$. LET $disc(K) = disc_K(\alpha_1, \dots, \alpha_n)$. THUS $disc_K(\alpha, \alpha_2, \dots, \alpha_n) = r_1^2 d$. SINCE $p \nmid r_1$, IT SUFFICES TO SHOW THAT $p \mid disc_K(\alpha, \alpha_2, \dots, \alpha_n)$. NOTICE THAT $\alpha \in$ EVERY PRIME OF $\mathcal{O}_L$ LYING OVER p (SINCE THEY LIE OVER THE PRIMES OF $\mathcal{O}_K$ LYING OVER p). FIX $\mathfrak{q} \subset \mathcal{O}_L$, $\mathfrak{q} \cap \mathbb{Q} = p$

THEN $\alpha \in \mathfrak{q}$. WE CLAIM THAT $\prec(\alpha) \in \mathfrak{q}$. NOTICE THAT $\prec^{-1}(\mathfrak{q})$ IS ALSO A PRIME OF

$\mathcal{O}_L$ LYING OVER $p \Rightarrow \alpha \in \sigma^{-1}(\mathcal{Q}) \Rightarrow \sigma(\alpha) \in \mathcal{Q}$ $\forall \sigma \Rightarrow \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in \mathcal{Q}$ AND $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in \mathbb{Z} \Rightarrow \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in p\mathbb{Z}$ #

Cor ONLY FINITELY MANY PRIMES IN $\mathbb{Z}$ ARE RAMIFIED IN $\mathcal{O}_K$.

Cor LET $K \subseteq L$ BE NUMBER FIELDS. ONLY FINITELY MANY PRIMES OF $\mathcal{O}_K$ ARE RAMIFIED IN $\mathcal{O}_L$.

Proof: TAKE $\mathfrak{P} \subseteq \mathcal{O}_K$ RAMIFIED. THEN $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$ IS RAMIFIED IN $\mathcal{O}_L$. THERE ARE FINITELY MANY SUCH p's $\Rightarrow$ THERE ARE FINITELY MANY SUCH $\mathfrak{P}$'s #

LET $K \subseteq L$ BE NUMBER FIELDS WITH $n = [L:K]$. FIX $\alpha \in \mathcal{O}_L$ OF DEGREE n OVER K SO THAT $L = K(\alpha)$. THEN $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$ AND $\mathcal{O}_L / \mathcal{O}_K[\alpha]$ IS A FINITE GROUP SINCE BOTH $\mathcal{O}_L$ AND $\mathcal{O}_K[\alpha]$ ARE FREE ABELIAN OF RANK $n = [K:\mathbb{Q}]$.

FOR ALL BUT FINITELY MANY $\mathfrak{P}$ OF $\mathcal{O}_K$, THE SPLITTING OF $\mathfrak{P}$ IN $\mathcal{O}_L$ CAN BE DETERMINED BY FACTORING A CERTAIN POLYNOMIAL MODULO $\mathfrak{P}$. THIS IS PROVIDED THAT $p \nmid |\mathcal{O}_L / \mathcal{O}_K[\alpha]|$ FOR $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$.

FIX $\mathfrak{P} \subseteq \mathcal{O}_K$, $h(x) \in \mathcal{O}_K[x]$, AND LET $\overline{h}(x)$ BE THE POLYNOMIAL IN $\mathcal{O}_K/\mathfrak{P}[x]$ OBTAINED BY REDUCING THE COEFFICIENTS OF $h(x)$ MODULO $\mathfrak{P}$.

LET $m_\alpha(x)$ BE THE MINIMAL POLYNOMIAL OF α OVER K. $m_\alpha(x) \in \mathcal{O}_K[x]$

WRITE $\overline{m_\alpha}(x) = \overline{m_1}(x)^{e_1} \cdots \overline{m_r}(x)^{e_r}$ IN $\mathcal{O}_K/\mathfrak{P}[x]$, WHERE THE $\overline{m_i}(x)$ ARE DISTINCT AND MONIC

THM (*) WITH EVERYTHING AS ABOVE, AND $p \nmid |\mathcal{O}_L / \mathcal{O}_K[\alpha]|$ FOR p LYING UNDER $\mathfrak{P}$ THEN $\mathfrak{P}\mathcal{O}_L = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_r^{e_r}$, WHERE

$\mathcal{Q}_i = (\mathfrak{P}, m_i(\alpha)) = \mathfrak{P}\mathcal{O}_L + (m_i(\alpha))$, $f(\mathcal{Q}_i/\mathfrak{P}) = \deg m_i$.

Ex CONSIDER $\mathbb{Q}(\sqrt{\ell}) = L$, WITH ℓ SQUARE-FREE. WE HAVE $\mathbb{Z}[\sqrt{\ell}] \subseteq \mathcal{O}_L$

$$|\mathcal{O}_L / \mathbb{Z}[\sqrt{\ell}]| = \begin{cases} 1 & \text{IF } \ell \equiv 2,3 \pmod 4 \\ 2 & \text{IF } \ell \equiv 1 \pmod 4 \end{cases}$$

THM IF $p \mid \ell \Rightarrow p\mathcal{O}_L = (p, \sqrt{\ell})^2$

IF ℓ IS ODD, $2\mathcal{O}_L = \begin{cases} (2, 1+\sqrt{\ell})^2 & \text{IF } \ell \equiv 3 \pmod 4 \\ \left(2, \frac{1+\sqrt{\ell}}{2}\right)\left(2, \frac{1-\sqrt{\ell}}{2}\right) & \text{IF } \ell \equiv 1 \pmod 8 \\ \text{PRIME} & \text{IF } \ell \equiv 5 \pmod 8 \end{cases}$

IF p IS ODD, $p \nmid \ell$,

$$p\mathcal{O}_L = \begin{cases} (p, h+\sqrt{\ell})(p, h-\sqrt{\ell}) & \text{IF } \ell \equiv h^2 \pmod p \\ \text{PRIME IF } \ell \text{ NOT A SQUARE MOD } p \end{cases}$$

Proof $\alpha = \sqrt{\ell}$, $m(x) = x^2 - \ell$

IF $p = 2$, ℓ ODD $x^2 - \ell \equiv x^2 + 1 \equiv (x+1)^2 \pmod 2$

IF $\ell \equiv 3 \pmod 4$, THEN THEOREM ★ IMPLIES $2\mathcal{O}_L = (2, 1+\sqrt{\ell})^2$

IF $\ell \equiv 1 \pmod 4$, WE TAKE $\alpha = \frac{\sqrt{\ell}+1}{2}$, $m(x) = x^2 - x + \frac{1-\ell}{4} = \begin{cases} x(x+1) & \text{IF } \ell \equiv 1 \pmod 8 \\ x^2+x+1 & \text{IF } \ell \equiv 5 \pmod 8 \end{cases}$ (IRREDUCIBLE)

IF $\ell \equiv 1 \pmod 8$ $2\mathcal{O}_L = \left(2, \frac{\sqrt{\ell}+1}{2}\right)\left(2, \frac{1+\sqrt{\ell}}{2}\right)$

IF ℓ EVEN, $x^2 - \ell \equiv x^2 \pmod 2$ $\quad 2\mathcal{O}_L = (2, \sqrt{\ell})^2$

THE CASE $p \mid \ell$ IS SIMILAR.

IF p ODD, $p \nmid \ell$ $x^2 - \ell = \begin{cases} (x-u)(x+u) & \text{IF } \ell \equiv u^2 \pmod p \\ \text{IRREDUCIBLE} & \text{IF } \ell \text{ NOT A SQUARE MOD } p \end{cases}$ ★★

PROOF OF THEOREM ★ LET $f_i = \deg m_i = \deg \overline{m_i}$. WE PROVE

① FOR EACH i, $\mathcal{Q}_i = \mathcal{O}_L$ OR $\mathcal{O}_L/\mathcal{Q}_i$ IS A FIELD OF ORDER $|\mathcal{O}_K/\mathcal{P}|^{f_i}$

② $\mathcal{Q}_i + \mathcal{Q}_j = \mathcal{O}_L$ $i \neq j$

③ $\mathcal{P}\mathcal{O}_L \mid \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_r^{e_r}$

ASSUME ①, ②, ③. REARRANGING, WE CAN ASSUME $\mathcal{Q}_1, \dots, \mathcal{Q}_s \neq \mathcal{O}_L$, $\mathcal{Q}_{s+1}, \dots, \mathcal{Q}_r = \mathcal{O}_L$. WE HAVE $\mathcal{Q}_i \cap \mathcal{O}_K \supseteq \mathcal{P} \Rightarrow \mathcal{Q}_i$ PRIME IDEAL OF $\mathcal{O}_L$ LYING OVER $\mathcal{P}$ FOR $i = 1, \dots, s$. WE ALSO HAVE $|\mathcal{O}_L/\mathcal{Q}_i| = |\mathcal{O}_K/\mathcal{P}|^{f_i}$ IMPLIES $f(\mathcal{Q}_i \mid \mathcal{P}) = f_i$ $i = 1, \dots, s$

BY ②, THE $\mathcal{Q}_i$ ARE DISTINCT FOR $i = 1, \dots, s$.

BY ③, $\mathcal{P}\mathcal{O}_L \mid \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_s^{e_s} \Rightarrow \mathcal{P}\mathcal{O}_L = \mathcal{Q}_1^{d_1} \cdots \mathcal{Q}_s^{d_s}$ WITH $d_i \leq e_i \Rightarrow \sum_{i=1}^{s} d_i f_i = n$. ON THE OTHER HAND, $n = \deg m = \sum_{i=1}^{r} e_i f_i \Rightarrow r = s$, AND $d_i = e_i$.

PROOF OF ① TAKE $F_i = (\mathcal{O}_K/\mathcal{P})[x]/(\overline{m_i})$. F_i IS A FIELD OF $|\mathcal{O}_K/\mathcal{P}|^{f_i}$ ELEMENTS. CONSIDER $\varphi_i : \mathcal{O}_K[x] \to F_i$ THE REDUCTION MOD $\mathcal{P}$ AND MOD $\overline{m_i}$ MAP. IT IS ONTO. ITS KERNEL IS $\varphi_i(h) = 0$ $\Leftrightarrow h \in (\overline{m_i}) \Leftrightarrow h = f\overline{m_i}$ FOR SOME $f \in \mathcal{O}_K[x] \Leftrightarrow h - f m_i \in \mathcal{P}[x]$ (HERE WE MEAN $\mathcal{P}[x] = \mathcal{P}\mathcal{O}_K[x]$) $\Leftrightarrow h \in (\mathcal{P}[x], m_i)$ $\Rightarrow \mathcal{O}_K[x]/(\mathcal{P}[x], m_i) \cong (\mathcal{O}_K/\mathcal{P})[x]/(\overline{m_i}) \Rightarrow (\mathcal{P}[x], m_i)$ MAXIMAL IDEAL.

NOW CONSIDER $\mathcal{O}_K[x] \to \mathcal{O}_L$ AND $\psi_i : \mathcal{O}_K[x] \to \mathcal{O}_L/\mathcal{Q}_i$

$x \to \alpha$

THEN $(\mathcal{P}[x], m_i) \subseteq \ker \psi_i$. THIS IMPLIES $\ker \psi_i = \mathcal{O}_K[x]$ OR $\ker \psi_i = (\mathcal{P}[x], m_i)$. WE PROVE THAT ψ_i IS ONTO. WE HAVE TO SHOW THAT $\mathcal{O}_L = \mathcal{O}_K[\alpha] + \mathcal{Q}_i$. WE KNOW THAT $p \in \mathcal{P} \subseteq \mathcal{Q}_i \Rightarrow p\mathcal{O}_L \subseteq \mathcal{Q}_i$

SINCE $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ AND THE INDEX OF $\mathcal{O}_K[\alpha] + p\mathcal{O}_L$ MUST BE A COMMON DIVISOR OF $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ AND $|\mathcal{O}_L/p\mathcal{O}_L|$ AND THEY ARE COPRIME SINCE $|\mathcal{O}_L/p\mathcal{O}_L|$ IS A POWER OF p, WE CONCLUDE THAT

$\mathcal{O}_L = \mathcal{O}_K[\alpha] + p\mathcal{O}_L = \mathcal{O}_K[\alpha] + \mathcal{Q}_{ij}$. THUS ψ_{ij} IS ONTO $\Rightarrow$

$\mathcal{O}_K[x]/\ker\psi_{ij} \simeq \mathcal{O}_L/\mathcal{Q}_{ij}$. IF $\ker\psi_{ij} = (\mathcal{P}[x], m_{ij})$, WE GET

$\mathcal{O}_L/\mathcal{Q}_{ij} \simeq \mathcal{O}_K[x]/(\mathcal{P}[x], m_{ij}) \simeq F_{ij}$

PROOF OF ② WE HAVE THAT $\overline{m}_{ij}$, $\overline{m}_{ij}$ ARE DISTINCT AND IRREDUCIBLES, $\Rightarrow$

$\exists\, h, k \in \mathcal{O}_K/\mathcal{P}[x]$ SUCH THAT $\overline{m}_{ij}h + \overline{m}_{ij}k = 1 \Rightarrow$

$m_{ij}h + m_{ij}k \equiv 1 \pmod{\mathcal{P}[x]} \Rightarrow m_{ij}(\alpha)h(\alpha) + m_{ij}(\alpha)k(\alpha) \equiv 1 \pmod{\mathcal{P}\mathcal{O}_L}$

SINCE $\mathcal{P}[\alpha] \subseteq \mathcal{P}\mathcal{O}_L$. $\Rightarrow 1 \in (\mathcal{P}, m_{ij}(\alpha), m_{ij}(\alpha)) = \mathcal{Q}_{ij} + \mathcal{Q}_{ij}$

PROOF OF ③ RECALL THAT $\mathcal{Q}_{ij} = (\mathcal{P}, m_{ij}(\alpha))$.

$\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_r^{e_r} \subseteq (\mathcal{P}, m_1(\alpha)^{e_1}\cdots m_r(\alpha)^{e_r}) \doteq \mathcal{P}\mathcal{O}_L$

WE NEED TO PROVE THAT $m_1(\alpha)^{e_1}\cdots m_r(\alpha)^{e_r} \in \mathcal{P}\mathcal{O}_L$ — WE WANT TO PROVE THIS

SINCE $\overline{m}_1^{e_1}\cdots\overline{m}_r^{e_r} = \overline{m}$, THEN $m_1^{e_1}\cdots m_r^{e_r} \equiv m \pmod{\mathcal{P}[x]} \Rightarrow$

$m_1(\alpha)^{e_1}\cdots m_r(\alpha)^{e_r} \equiv m(\alpha) = 0 \pmod{\mathcal{P}\mathcal{O}_L} \Rightarrow \mathcal{P}\mathcal{O}_L \mid \mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_r^{e_r}$ #