Number Fields and Number Rings

Def An **algebraic number** is a root of a nonzero polynomial in $\mathbb{Q}[x]$

Prop An element α of a field extension of $\mathbb{Q}$ is an algebraic number iff the ring $\mathbb{Q}[\alpha]$ is a finite dimensional $\mathbb{Q}$-vector space.

Proof: Suppose that α is algebraic. Then there is $f(x)\in\mathbb{Q}[x]$ such that $f(\alpha)=0$, $f(x)=a_n x^n+\dots+a_0=0 \Rightarrow \alpha^n=-\frac{1}{a_n}(a_{n-1}\alpha^{n-1}+\dots+a_0)$ $\Rightarrow \alpha^n\in\langle 1,\alpha,\dots,\alpha^{n-1}\rangle_{\mathbb{Q}}$, $\alpha^{n+1}\in\langle\alpha,\alpha^2,\dots,\alpha^n\rangle_{\mathbb{Q}}=\langle 1,\alpha,\alpha^2,\dots,\alpha^{n-1}\rangle_{\mathbb{Q}}$, etc. Now suppose $\mathbb{Q}[\alpha]$ has finite dimension. Then $\exists\, n$ such that $\alpha^n\in\langle 1,\alpha,\dots,\alpha^{n-1}\rangle$. Then α satisfies a polynomial of $\deg=n$ #

Prop: Let k be a field, $\alpha,\beta\in k$ algebraic numbers. Then $\alpha\beta$, $\alpha\pm\beta$ are algebraic numbers.

Proof: Let f,g polynomials such that $f(\alpha)=0$, $g(\beta)=0$, $\deg f=m$, $\deg g=n$. Then $\mathbb{Q}[\alpha\beta]\subseteq k$ is a $\mathbb{Q}$-vector space spanned by $\alpha^i\beta^j$, $0\le i\le m-1$, $0\le j\le n-1$. Thus $\mathbb{Q}[\alpha,\beta]$ has finite dimension, $\mathbb{Q}[\alpha+\beta]$, $\mathbb{Q}[\alpha\beta]\subseteq\mathbb{Q}[\alpha,\beta]$ are subspaces $\Rightarrow \alpha+\beta$, $\alpha\beta$ are algebraic numbers #

Lemma If α is algebraic and $\gamma\in\mathbb{Q}[\alpha]$, $\gamma\neq 0$, then $\gamma^{-1}\in\mathbb{Q}[\alpha]$.

Proof: Since $\mathbb{Q}[\gamma]\subseteq\mathbb{Q}[\alpha]$ has finite dimension, then γ is algebraic. $\exists\, a_{n-1},\dots,a_0\in\mathbb{Q}$, such that $\gamma^n+a_{n-1}\gamma^{n-1}+\dots+a_0=0$. We can suppose $a_0\neq 0$. Then $\gamma^{-1}=-\frac{1}{a_0}(\gamma^{n-1}+\dots+a_1)\in\mathbb{Q}[\alpha]$ #

Obs For α algebraic, $\mathbb{Q}[\alpha]$ is a field. $\mathbb{Q}[\alpha]=\mathbb{Q}(\alpha)$.

Notation We denote by $\overline{\mathbb{Q}}$ the field of algebraic numbers.

Def An $\alpha\in\overline{\mathbb{Q}}$ is an **algebraic integer** if it is a root of a **monic** polynomial with coefficients in $\mathbb{Z}$. We also say that α is **integral**.

Ex $\sqrt{2}$ root of x^2-2 is an algebraic integer, but $\frac{1}{\sqrt{2}}$ is not because it is root of $2x^2-1$ (non-monic, we will prove this later)

Prop Let $\alpha\in\overline{\mathbb{Q}}$. Then α is an algebraic integer iff $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

Proof $\Rightarrow$) Clear $\Leftarrow$) Suppose that $\alpha\in\overline{\mathbb{Q}}$ and that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. We have $\mathbb{Z}[\alpha]=\langle f_1(\alpha),\dots,f_n(\alpha)\rangle_{\mathbb{Z}}$. Let $d>\max\deg f_i$. Then $\exists\, a_i$ such that $\alpha^d=\sum_{i=0}^{n} a_i f_i(\alpha)$. Thus α is root of $x^d-\sum_{i=0}^{n} a_i f_i(x)\in\mathbb{Z}[x]$, a monic polynomial. Then α is an algebraic integer #

Prop: Let $\alpha,\beta\in\overline{\mathbb{Q}}$ algebraic integers. Then $\alpha\beta$, $\alpha+\beta$ are also algebraic

INTEGERS.

PROOF: LET f,g MONIC POLYNOMIALS SUCH THAT $f(\alpha)=0$, $g(\beta)=0$, $\deg f=m$, $\deg g=n$. THE ELEMENTS $\alpha^i\beta^j$, $0\le i\le m-1$, $0\le j\le n-1$ SPAN THE $\mathbb{Z}$-MODULE $\mathbb{Z}[\alpha,\beta]$. NOTICE THAT $\mathbb{Z}[\alpha+\beta]$, $\mathbb{Z}[\alpha\beta]$ ARE SUBMODULES OF $\mathbb{Z}[\alpha,\beta]$ WHICH IS FINITELY GENERATED OVER THE NOETHERIAN RING $\mathbb{Z}$, AND THEREFORE $\mathbb{Z}[\alpha,\beta]$ IS NOETHERIAN AND BOTH $\mathbb{Z}[\alpha+\beta]$ AND $\mathbb{Z}[\alpha\beta]$ ARE FINITELY GENERATED. $\Rightarrow$ $\alpha+\beta$, $\alpha\beta$ INTEGRAL #

DEF: THE RING OF ALGEBRAIC INTEGERS OF $\overline{\mathbb{Q}}$ IS DENOTED BY $\overline{\mathbb{Z}}$.

MINIMAL POLYNOMIAL

DEF A (THE) MINIMAL POLYNOMIAL OF $\alpha\in\overline{\mathbb{Q}}$ IS A MONIC POLYNOMIAL $f\in\mathbb{Q}[x]$ OF MINIMAL DEGREE SUCH THAT $f(\alpha)=0$

LEMMA. SUPPOSE $\alpha\in\overline{\mathbb{Q}}$. THEN A MINIMAL POLYNOMIAL OF α DIVIDES ANY POLYNOMIAL $h(x)$ SUCH THAT $h(\alpha)=0$

PROOF: LET $m(x)$ BE A MINIMAL POLYNOMIAL OF α. BY THE DIVISION ALGORITHM $h(x)=m(x)q(x)+r(x)$, WHERE $r(x)=0$ OR $\deg r<\deg m$. SINCE $h(\alpha)=0$ AND $m(\alpha)=0$, WE GET $r(\alpha)=0$ BUT $\deg m$ IS MINIMAL $\Rightarrow$ $r(x)=0$ $\Rightarrow$ $m(x)\mid h(x)$ IN $\mathbb{Q}[x]$ #

COR: THE MINIMAL POLYNOMIAL IS UNIQUE. WE WRITE $m_\alpha(x)$

EX THE MINIMAL POLYNOMIAL OF $\sqrt{2}+3$ IS x^2-6x+7.

LEMMA: SUPPOSE $\alpha\in\mathbb{Q}$. THEN α IS AN ALGEBRAIC INTEGER IFF $m_\alpha(x)\in\mathbb{Z}[x]$

PROOF $\Leftarrow$) CLEAR $\Rightarrow$) SUPPOSE THAT α IS AN ALGEBRAIC INTEGER. THEN THERE IS $h(x)\in\mathbb{Z}[x]$ MONIC SUCH THAT $h(\alpha)=0$. BY THE PREVIOUS LEMMA, $h(x)=m_\alpha(x)q(x)$ FOR SOME $q(x)\in\mathbb{Q}[x]$. SINCE $h(x)$, $m_\alpha(x)$ MONIC, WE HAVE THAT $q(x)$ IS MONIC. IF $m_\alpha(x)\notin\mathbb{Z}[x]$, $\exists p$ PRIME THAT DIVIDES THE DENOMINATOR OF A COEFFICIENT OF $m_\alpha(x)$. LET p^i BE THE LARGEST POWER DIVIDING SUCH DENOMINATORS OF $m_\alpha(x)$ AND p^j BE THE LARGEST POWER DIVIDING SUCH DENOMINATORS OF $q(x)$. THEN $p^{i+j}h=(p^im_\alpha)(p^jq)$. REDUCING BOTH SIDES MODULO p, THE LEFT-HAND SIDE IS 0 AND THE RIGHT-HAND SIDE IS NOT. THIS IS A CONTRADICTION. THEN $m_\alpha(x)\in\mathbb{Z}[x]$ #

EX $\frac{1}{\sqrt{2}}$ IS NOT AN ALGEBRAIC INTEGER BECAUSE ITS MINIMAL POLYNOMIAL IS $x^2-\frac{1}{2}$

EX THE ONLY ALGEBRAIC INTEGERS IN $\mathbb{Q}$ ARE THE ELEMENTS OF $\mathbb{Z}$.

Ex $\frac{1+\sqrt{5}}{2}$ is an algebraic integer because it is root of x^2-x-1

Cyclotomic Fields

Algebraic Number Theory

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

M. Lalín

Let $\omega_r = e^{2\pi i/r}$ and let $\phi_r(x)$ be the minimal polynomial of ω_r. We have $\phi_r(x) \mid x^r-1$. Any root of $\phi_r(x)$ has the form ω_r^k. Moreover, we must have $(k,r)=1$, since otherwise we would have $\phi_r(x) \mid x^s-1$ with some $s<r$, but $\omega_r^s \neq 1$.

Thm: All ω_r^k, $1 \leq k \leq r$, $(k,r)=1$ are roots of $\phi_r(x)$.

Proof: We will prove that for any prime p, $p \nmid r$, $\phi_r(\omega_r^p)=0$.

We have $x^r-1 = \phi_r(x) g(x)$ with $\phi_r(x), g(x) \in \mathbb{Z}[x]$ (since ω_r integral and $\phi_r(x) \in \mathbb{Z}[x]$). Suppose ω_r^p is not a root of $\phi_r(x)$. Then ω_r^p is a root of $g(x) \Rightarrow \phi_r(x) \mid g(x^p)$ in $\mathbb{Q}[x]$. We write $g(x^p) = \phi_r(x) h(x)$ in $\mathbb{Z}[x]$ (as in previous lemma). We reduce modulo p and get $\overline{g(x)}^p \equiv \overline{\phi_r(x)}\,\overline{h(x)} \pmod p$. By unique factorization in $\mathbb{F}_p[x]$ there is a common factor of $\overline{g}$ and $\overline{\phi_r}$, say $\overline{\ell(x)}$, such that $\overline{\ell(x)}^2 \mid \overline{g(x)}\,\overline{\phi_r(x)} = \overline{x^r-1} \Rightarrow \overline{\ell(x)} \mid (\overline{x^r-1})' = \overline{r x^{r-1}}$. Since $p \nmid r$, $\bar{r} \neq 0$ $\Rightarrow \overline{\ell(x)}$ is a monomial, but this is impossible since $\overline{\ell(x)} \mid \overline{x^r-1}$. Then ω_r^p is a root of $\phi_r(x)$ $\forall p \nmid r$ #

Coro $\deg \phi_r(x) = \varphi(r)$, where $\varphi(r) = \#\{1 \leq k \leq r \mid (k,r)=1\}$ is Euler's totient function.

Coro. The Galois group of $\mathbb{Q}[\omega_r]/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^* = \{1 \leq k \leq r \mid (k,r)=1\}$ (multiplicative group of $\mathbb{Z}/r\mathbb{Z}$)

Proof: Each automorphism of $\mathbb{Q}(\omega_r)$ is determined by the image of ω_r, which must be a root of $\phi_r(x)$. Thus the possible images are ω_r^k with $1 \leq k \leq r$, $(k,r)=1$. The composition is given by multiplication modulo r #

Notice that the subfields of $\mathbb{Q}(\omega_r)$ correspond to subgroups of $(\mathbb{Z}/r\mathbb{Z})^*$. If p is prime, $\mathbb{Q}(\omega_p)$ contains a unique subfield for each degree dividing $p-1$ (because $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$). Thus, for p odd, $\mathbb{Q}(\omega_p)$ contains a unique quadratic field. This is $\mathbb{Q}(\sqrt{\pm p})$ with a sign depending on p.

Coro If r is even, the only roots of 1 in $\mathbb{Q}(\omega_r)$ are the r^{th} roots of 1. If r is odd, the only roots of 1 in $\mathbb{Q}(\omega_r)$ are the $2r^{\text{th}}$ roots

Proof: We can assume that r is even. Let ζ be a primitive k^{th} root of 1

in $\mathbb{Q}(\omega_r)$. Then $\mathbb{Q}(\omega_r)$ contains a primitive d^{th} root with $d=[k,r]$

(write $\omega=e^{2\pi i/k}$ $(l,k)=1$, let $(r,k)=m$ $\exists\ a,b$ such that $\frac{r}{m}la+\frac{k}{m}b=1$. Then $\omega^{\alpha}\omega_r^{\beta}=e^{2\pi i\left(\frac{l\alpha}{k}+\frac{\beta}{r}\right)}=e^{\frac{2\pi i m}{kr}\left(\frac{lr\alpha}{m}+\frac{k\beta}{m}\right)}=e^{\frac{2\pi i}{d}}$)

Then $\mathbb{Q}(\omega_r)$ contains $\mathbb{Q}(\omega_d)\Rightarrow\varphi(d)\le\varphi(r)$ But $r\mid d$ implies

$$\varphi(d)=\varphi(r)\,\varphi\left(\frac{d}{r}\right)\frac{(r,\frac{d}{r})}{\varphi((r,\frac{d}{r}))}$$

and then $\varphi(\frac{d}{r})=1$, $(r,\frac{d}{r})=\varphi((r,\frac{d}{r}))$, $\frac{d}{r}=1,2$

This gives $(r,\frac{d}{r})=1$, and since r is even, we get $\frac{d}{r}=1\Rightarrow d=r$

$\Rightarrow k\mid r$ and ω is an r^{th} root of 1.

When r is odd, just consider $\mathbb{Q}(\omega_{2r})=\mathbb{Q}(\omega_r)$. #

Cor: The r^{th} cyclotomic fields, for r even, are all distinct and pairwise nonisomorphic.

Number Fields, Ring of Integers, Orders

Def: A **number field** is a field K that contains $\mathbb{Q}$ as a subfield and such that $[K:\mathbb{Q}]=\dim_{\mathbb{Q}}K$ is finite.

If K is a number field, the Primitive Element Theorem implies $K=\mathbb{Q}(\alpha)$ and $[K:\mathbb{Q}]=\deg m_{\alpha}(x)$

Def The **ring of integers** of a number field K is the ring

$$\mathcal{O}_K=\{x\in K:\ x \text{ is an algebraic integer}\}$$

Ex $K=\mathbb{Q}(i)$, $\mathcal{O}_K=\mathbb{Z}[i]$

Ex $r\in\mathbb{Z}$, r square-free.

$$\mathcal{O}_{\mathbb{Q}(\sqrt{r})}=\begin{cases}\mathbb{Z}[\sqrt{r}] & r\equiv 2,3\pmod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{r}}{2}\right] & r\equiv 1\pmod 4\end{cases}$$

Proof The elements of K are of the form $\alpha=a+b\sqrt{r}$, with $a,b\in\mathbb{Q}$.

because $[K:\mathbb{Q}]=2$. If $b\neq 0$, we have $x^2-2ax+(a^2-b^2r)$ monic and it must be irreducible since $\alpha\notin\mathbb{Q}$. If α is an algebraic integer, then $2a\in\mathbb{Z}$, $a^2-b^2r\in\mathbb{Z}$ Then $4a^2-4b^2r\in\mathbb{Z}\Rightarrow 4b^2r\in\mathbb{Z}$. Also $4a^2-4b^2r\equiv 0\pmod 4$

$\Rightarrow 4a^2\equiv 4b^2r\pmod 4$ If $r\not\equiv 1\pmod 4$, then $4a^2\equiv 4b^2\equiv 0\pmod 4$ (because $x^2\equiv 0,1\pmod 4$ for $x\in\mathbb{Z}$) $\Rightarrow a,b\in\mathbb{Z}$

If $r\equiv 1\pmod 4$, $4a^2\equiv 4b^2\pmod 4\equiv 0$ or $1\pmod 4$. If $4a^2\equiv 1\pmod 4$, $a=\frac{a'}{2}$, $a'\in\mathbb{Z}$, $b=\frac{b'}{2}$, $b'\in\mathbb{Z}$ $2\nmid a'b'$ Then $\alpha=\frac{a'+b'\sqrt{r}}{2}=\frac{a'-b'}{2}+b'\frac{1+\sqrt{r}}{2}$

$a'\equiv b'\pmod 2\Rightarrow\frac{a'-b'}{2}\in\mathbb{Z}$, $\alpha\in\mathbb{Z}\left[\frac{1+\sqrt{r}}{2}\right]$ #

Def An **order** in $\mathcal{O}_K$ is any subring with unit R of $\mathcal{O}_K$ such that

THE QUOTIENT $\mathcal{O}_K/R$ OF ABELIAN GROUPS IS FINITE

Ex $\mathbb{Z}\subseteq\mathbb{Z}[i]$ IS NOT AN ORDER, SINCE $\mathbb{Z}[i]/\mathbb{Z}\simeq\mathbb{Z}$.

$2\mathbb{Z}+i\mathbb{Z}\subseteq\mathbb{Z}[i]$ IS NOT AN ORDER BECAUSE IT IS NOT A RING WITH UNIT.

$\mathbb{Z}+2i\mathbb{Z}\subseteq\mathbb{Z}[i]$ IS AN ORDER, $\mathbb{Z}[i]/\mathbb{Z}+2i\mathbb{Z}\simeq\mathbb{Z}/2\mathbb{Z}$.

Ex IF $K=\mathbb{Q}(\alpha)$, α INTEGRAL, $\mathbb{Z}[\alpha]$ IS AN ORDER OF K; BUT FREQUENTLY $\mathbb{Z}[\alpha]\neq\mathcal{O}_K$ IF $[K:\mathbb{Q}]=n$, $\mathcal{O}_K$ IS A FREE MODULE OF RANK n OVER A PID $\mathbb{Z}[\alpha]$ IS A SUBMODULE WITH THE SAME RANK

LEMMA LET K BE A NUMBER FIELD, THEN $\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$ AND $\mathbb{Q}\mathcal{O}_K=K$

PROOF LET $\alpha\in\mathbb{Q}$ SINCE THE MINIMAL POLYNOMIAL IS $x-\alpha$, WE GET α IS AN ALGEBRAIC INTEGER IFF $\alpha\in\mathbb{Z}$.

NOW LET $\alpha\in K$ WE WANT TO SEE THAT $\alpha\in\mathbb{Q}\mathcal{O}_K$. CONSIDER $m_\alpha(x)\in\mathbb{Q}[x]$. IF $\ell\in\mathbb{Z}$, $\ell^{\deg m_\alpha}m_\alpha\left(\frac{x}{\ell}\right)$ IS THE MINIMAL POLYNOMIAL FOR $\ell\alpha$. IF WE TAKE ℓ TO BE THE LEAST COMMON MULTIPLE OF THE DENOMINATORS OF THE COEFFICIENTS OF m_α, THEN $\ell\alpha$ IS INTEGRAL; $\ell\alpha\in\mathcal{O}_K\Rightarrow$ $\alpha\in\mathbb{Q}\mathcal{O}_K=K$. $\#$

Function Fields

LET K BE ANY FIELD. WE CAN CONSIDER THE SAME DEFINITIONS WITH $\mathbb{Q}$ REPLACED BY $k(t)$ AND $\mathbb{Z}$ REPLACED BY $k[t]$. THE ANALOGUE OF NUMBER FIELD BECOMES FUNCTION FIELD. (THAT IS, A FINITE ALGEBRAIC EXTENSION OF $k(t)$). GEOMETRICALLY, IF $F(x,t)=0$ IS A POLYNOMIAL, IT DEFINES AN AFFINE (OR PROJECTIVE) CURVE C. THEN $k(t)[x]/(F(x,t))$ IS THE FIELD OF RATIONAL FUNCTIONS ON THE PROJECTIVE CLOSURE OF C (FUNCTION FIELD). ALSO $\mathcal{O}_K$ IS THE SUBRING OF RATIONAL FUNCTIONS THAT HAVE NO POLES IN THE AFFINE CURVE $F(x,t)=0$.

Norms and Traces

DEF LET $\alpha\in\overline{\mathbb{Q}}$. THE CONJUGATES OR GALOIS CONJUGATES OF α ARE THE ROOTS OF $m_\alpha(x)$.

Ex $\sqrt{2}$ HAS MINIMAL POLYNOMIAL x^2-2. ITS CONJUGATES ARE $\sqrt{2}$ AND $-\sqrt{2}$

$\sqrt[3]{2}$ HAS MINIMAL POLYNOMIAL x^3-2. ITS CONJUGATES ARE $\sqrt[3]{2}, \sqrt[3]{2}\omega_3, \sqrt[3]{2}\omega_3^2$

THE CONJUGATES OF ω_r ARE ω_r^k, $(k,r)=1$.

LET K BE A NUMBER FIELD $[K:\mathbb{Q}]=n$. WE KNOW THAT THERE ARE n EMBEDDINGS OF K IN $\overline{\mathbb{Q}}$ (OR $\mathbb{C}$).

The embeddings of $\mathbb{Q}(\alpha)$ in $\overline{\mathbb{Q}}$ are determined by the image of α, which can be sent to any of its n conjugates.

Let $k \subset L$ be number fields. We denote $[L:k] = \dim_k L$. Every embedding of k in $\overline{\mathbb{Q}}$ extends to $[L:k]$ embeddings of L in $\overline{\mathbb{Q}}$. In particular, L has $[L:k]$ embeddings in $\overline{\mathbb{Q}}$ that leave k fixed.

Def Let $\alpha \in L$. The **left multiplication by α** is $\ell_\alpha : L \to L$. It is a k-linear transformation.

Def The **norm** and **trace** of α from L to k are

$$N_{L/k}(\alpha) = \det(\ell_\alpha) \qquad \mathrm{Tr}_{L/k}(\alpha) = \mathrm{tr}(\ell_\alpha)$$

From linear algebra, we know

$$N_{L/k}(\alpha\beta) = N_{L/k}(\alpha) N_{L/k}(\beta)$$
$$\mathrm{Tr}_{L/k}(\alpha+\beta) = \mathrm{Tr}_{L/k}(\alpha) + \mathrm{Tr}_{L/k}(\beta)$$

If $f \in \mathbb{Q}[x]$ is the characteristic polynomial of ℓ_α, then the constant term is $(-1)^{\deg f} \det(\ell_\alpha)$ and the coefficient of $x^{\deg f - 1}$ is $-\mathrm{tr}(\ell_\alpha)$.

Prop: Let $\alpha \in L$, and let $\sigma_1, \dots, \sigma_d$ be the embeddings $L/k \hookrightarrow \overline{\mathbb{Q}}$ that fix k (here $d = [L:k]$). Then

$$N_{L/k}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) \qquad \mathrm{Tr}_{L/k}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha)$$

Proof: The minimal polynomial $m_\alpha(x)$ has distinct roots and it is irreducible. We have $k(\alpha) \cong k[x]/(m_\alpha)$ $[k(\alpha):k] = \deg m_\alpha$. If α satisfies a polynomial, so does ℓ_α. Then the characteristic polynomial of ℓ_α acting on $k(\alpha)$ is m_α. Let $b_1, \dots, b_n$ be a basis for $L/k(\alpha)$, and let $1, \alpha, \dots, \alpha^m$ be a basis for $k(\alpha)/k$. $m = \deg m_\alpha - 1$. Left multiplication by α acts in the same way on $b_i, \alpha b_i, \dots, \alpha^m b_i$ for any $1 \le i \le n$. Then the matrix of ℓ_α on L is a block direct sum of copies of the matrix of ℓ_α acting on $k(\alpha)$. Thus the characteristic polynomial of ℓ_α on L is $m_\alpha^{[L:k(\alpha)]}$. The proposition follows #

Ex $\mathrm{Tr}_{L/k}(1) = [L:k]$, 1 has $[L:k]$ conjugates equal to 1.

Ex $L = \mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}$

$\mathbb{Q}$-homomorphisms or embeddings

$\sigma_1 : \sqrt[4]{2} \to \sqrt[4]{2}$ $\sigma_2 : \sqrt[4]{2} \to \sqrt[4]{2}\, i$ $\sigma_3 : \sqrt[4]{2} \to -\sqrt[4]{2}$

$\sigma_4 : \sqrt[4]{2} \to -\sqrt[4]{2}\, i$

$$N_{L/\mathbb{Q}}(\sqrt[4]{2}) = \sqrt[4]{2}\,(\sqrt[4]{2}\,i)(-\sqrt[4]{2})(-\sqrt[4]{2}\,i) = -2 \qquad \mathrm{Tr}_{L/\mathbb{Q}}(\sqrt[4]{2}) = 0$$

$N_{L/\mathbb{Q}}(\sqrt[4]{2}) = \sqrt[4]{2}(-\sqrt[4]{2})\sqrt{2}(-\sqrt{2}) = 4 \quad Tr_{L/\mathbb{Q}}(\sqrt[4]{2}) = 0$

$N_{L/\mathbb{Q}}(\sqrt[4]{2}+1) = (\sqrt[4]{2}+1)^2(-\sqrt[4]{2}+1)^2 = (-1)^2 = 1 \quad Tr_{L/\mathbb{Q}}(\sqrt[4]{2}+1) = 2((+\sqrt[4]{2})+(1-\sqrt[4]{2})) = 4$

EXTENSIONS $k = \mathbb{Q}(\sqrt[4]{2})$ $\sqrt[4]{2} \to \sqrt[4]{2}$ EXTENDS TO $\sqrt[4]{2} \to \sqrt[4]{2}$, $\to -\sqrt[4]{2}$.

$\sqrt[4]{2} \to -\sqrt[4]{2}$ EXTENDS TO $\sqrt[4]{2} \to \sqrt[4]{2}i$, $\to -\sqrt[4]{2}i$

NOTICE THAT THE EMBEDDINGS σ_1, σ_3 TAKE $\mathbb{Q}(\sqrt[4]{2})$ INTO ITSELF, BUT σ_2, σ_4 TAKE IT TO $\mathbb{Q}(\sqrt[4]{2}i)$. BUT IF WE CONSIDER THE LARGER FIELD $\mathbb{Q}(\sqrt[4]{2}, i)$, ALL THE EMBEDDINGS TAKE $\mathbb{Q}(\sqrt[4]{2}, i)$ TO ITSELF.

THIS PROPERTY IS CALLED BEING A **GALOIS EXTENSION**. ALL FIELDS HAVE A MINIMAL GALOIS EXTENSION CALLED THE **GALOIS CLOSURE**. FOR NUMBER FIELDS, THE GALOIS CLOSURE IS ANOTHER NUMBER FIELD.

Coro: LET $K \subseteq L \subseteq M$ BE A TOWER OF NUMBER FIELDS. THEN

$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)) \qquad Tr_{M/K}(\alpha) = Tr_{L/K}(Tr_{M/L}(\alpha))$$

Proof: SUPPOSE THAT $\sigma: L \hookrightarrow \overline{\mathbb{Q}}$ AND $\sigma': M \hookrightarrow \overline{\mathbb{Q}}$ EXTENDS σ (THERE ARE $[M:L]$ POSSIBLE σ') LET $\tau_1, \dots, \tau_d : M/L \hookrightarrow \overline{\mathbb{Q}}$ (FIXING L). WE WANT TO COMPOSE σ' WITH THE τ_i, BUT FOR THIS WE NEED A GALOIS EXTENSION. SO TAKE $\widetilde{M}$ THE GALOIS CLOSURE OF M. AND FIX EXTENSIONS OF $\sigma', \tau_1, \dots, \tau_d : \widetilde{M} \to \widetilde{M}$. WE GET THAT $\sigma'\tau_1, \dots, \sigma'\tau_d$ ARE EXTENSIONS OF σ. THUS

$$N_{L/K}(N_{M/L}(\alpha)) = N_{L/K}\left(\prod_{i=1}^{d} \tau_i(\alpha)\right) = \prod_{j=1}^{e} \sigma_j'\left(\prod_{i=1}^{d} \tau_i(\alpha)\right) =$$

$$= \prod \sigma_j' \tau_i(\alpha) = N_{M/K}(\alpha)$$

AND SIMILARLY FOR THE TRACE.

WE SHOULD CHECK THAT $\sigma_{j_1}'\tau_{i_1}|_M = \sigma_{j_2}'\tau_{i_2}|_M \Rightarrow \forall \alpha \in L \ \sigma_{j_1}'\tau_{i_1}(\alpha) = \sigma_{j_2}'\tau_{i_2}(\alpha)$

$\overset{\tau_i(\alpha)=\alpha \text{ IF } \alpha \in L}{\Rightarrow} \sigma_{j_1}'(\alpha) = \sigma_{j_2}'(\alpha) \Rightarrow \sigma_{j_1}' = \sigma_{j_2}' \Rightarrow \tau_{i_1} = \tau_{i_2}$

THUS, ALL THE COMPOSITIONS ARE DIFFERENT. AND THE NUMBER OF EMBEDDINGS IS CORRECT $\#$.

Obs $\alpha \in \mathcal{O}_L \Rightarrow N_{L/K}(\alpha), Tr_{L/K}(\alpha) \in \mathcal{O}_K$.

DISCRIMINANTS OF AN r-TUPLE

LET $K \subseteq L$ BE NUMBER FIELDS, $r = [L:K]$, AND LET $\sigma_1, \dots, \sigma_r$ BE EMBEDDINGS $L/K \hookrightarrow \overline{\mathbb{Q}}$

Def LET $\alpha_1, \dots, \alpha_r \in L$. THEN THE **DISCRIMINANT** OF $\alpha_1, \dots, \alpha_r$ IS

$$disc_{L/K}(\alpha_1, \dots, \alpha_r) = \det(\sigma_i(\alpha_j))^2$$

THM We have $\operatorname{disc}_{L/K}(\alpha_1,\dots,\alpha_r)=\det\left(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)\right)$

PROOF: Consider $\begin{pmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_r(\alpha_1)\\ \vdots&&\vdots\\ \sigma_1(\alpha_r)&\cdots&\sigma_r(\alpha_r)\end{pmatrix}\begin{pmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_1(\alpha_r)\\ \vdots&&\vdots\\ \sigma_r(\alpha_1)&\cdots&\sigma_r(\alpha_r)\end{pmatrix}$

$=\left(\sum_{k=1}^r\sigma_k(\alpha_i\alpha_j)\right)=\left(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)\right)$ ✓

COR We have $\operatorname{disc}_{L/K}(\alpha_1,\dots,\alpha_r)\in K$. If, in addition, $\alpha_i\in\mathcal{O}_L$, then $\operatorname{disc}_{L/K}(\alpha_1,\dots,\alpha_r)\in\mathcal{O}_K$.

THM $\operatorname{disc}_{L/K}(\alpha_1,\dots,\alpha_r)=0$ iff $\alpha_1,\dots,\alpha_r$ are linearly dependent over K

PROOF If the α_j are linearly dependent over K, so are the columns $(\sigma_i(\alpha_j))_{j=1,\dots,r}$. And $\operatorname{disc}(\sigma_i(\alpha_j))=0$.

If $\operatorname{disc}_{L/K}(\alpha_1,\dots,\alpha_r)=0$, then the rows of $(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j))$ are dependent. Let $a_1,\dots,a_r\in K$ such that

(*) $\sum_{k=1}^r a_k\operatorname{Tr}_{L/K}(\alpha_k\alpha_j)=0\ \forall j$.

Take $\alpha=\sum_{k=1}^r a_k\alpha_k$. Suppose that the α_j are linearly independent. Then $\alpha\neq0$. Now (*) implies $\operatorname{Tr}_{L/K}(\alpha\alpha_j)=0\ \forall j$

Since the α_j are a basis of L/K and $\alpha\neq0$, we get $\alpha\alpha_1,\dots,\alpha\alpha_r$ is also a basis of L/K. But then $\operatorname{Tr}_{L/K}(\beta)=0\ \forall\beta\in L\Rightarrow$ $\operatorname{Tr}_{L/K}(1)=0$. This is a contradiction since $\operatorname{Tr}_{L/K}(1)=r$ ✓

THM Let $L=K(\alpha)$, K number field, and let $\alpha_1,\dots,\alpha_r$ be the conjugates of α over K, with $m_{\alpha,K}(x)$ the minimal polynomial of α over K. Then

$$\operatorname{disc}_{L/K}(\alpha):=\operatorname{disc}_{L/K}(1,\alpha,\dots,\alpha^{r-1})=\prod_{1\le s<t\le r}(\alpha_t-\alpha_s)^2=(-1)^{\frac{r(r-1)}{2}}N_{L/K}(m'_{\alpha,K}(\alpha))$$

PROOF The first inequality follows from

$$\det\left(\sigma_k(\alpha^{j-1})\right)^2=\det\left(\sigma_k(\alpha)^{j-1}\right)^2=\det\left(\alpha_k^{j-1}\right)^2=\prod_{1\le s<t\le r}(\alpha_t-\alpha_s)^2$$

by the Van der Monde identity.

Now use $\prod_{1\le s<t\le r}(\alpha_t-\alpha_s)^2=(-1)^{\frac{r(r-1)}{2}}\prod_{s\neq t}(\alpha_s-\alpha_t)$

$$N_{L/K}(m'_{\alpha,K}(\alpha))=\prod_{s=1}^r\sigma_s(m'_{\alpha,K}(\alpha))=\prod_{s=1}^r m'_{\alpha,K}(\sigma_s(\alpha))=\prod_{s=1}^r m'_{\alpha,K}(\alpha_s)$$
$$=\prod_{s\neq t}(\alpha_s-\alpha_t)$$ ✓

EX Compute $\operatorname{disc}(\omega_p)=\operatorname{disc}(1,\omega_p,\dots,\omega_p^{p-2})$, $\omega_p=e^{2\pi i/p}$, p odd prime.

We have $x^p-1=(x-1)\phi_p(x)$. Differentiating, $px^{p-1}=\phi_p(x)+(x-1)\phi_p'(x)$

$\Rightarrow \phi_p'(\omega_p)=\frac{p}{\omega_p(\omega_p-1)} \Rightarrow N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\phi_p'(\omega_p))=\frac{N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(p)}{N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\omega_p)\,N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\omega_p-1)}=p^{p-1}$

Since $x^{p-1}+\cdots+1=(x-\omega_p)(x-\omega_p^2)\cdots(x-\omega_p^{p-1})$

$\Rightarrow N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(1-\omega_p)=p=N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\omega_p-1)$

Then $N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\phi_p'(\omega_p))=p^{p-2} \Rightarrow disc(\omega_p)=\begin{cases} p^{p-2} & p\equiv 1 \pmod 4 \\ -p^{p-2} & p\equiv 3 \pmod 4 \end{cases}$

The Additive Structure of $\mathcal{O}_K$

A **free abelian group** of rank r is a group isomorphic to $\mathbb{Z}^r$. If A,B,C are groups $A\leq B\leq C$ and A,C are free abelian of rank r, then B is also free abelian of rank r. (Ex 24, page 44, Marcus)

If K is a number field, we can choose a basis of algebraic integers $K=\langle \alpha_1,\dots,\alpha_r\rangle_{\mathbb{Q}}$ (because $K=\mathbb{Q}\mathcal{O}_K$). We want to prove that $\mathcal{O}_K$ is free abelian of rank r.

Thm Let $\{\alpha_1,\dots,\alpha_r\}$ a basis for $K/\mathbb{Q}$ with α_i integral. Let $d=disc_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_r)$. Then for $\alpha\in\mathcal{O}_K$, $\exists m_i\in\mathbb{Z}$, $d\mid m_i^2$ such that $\alpha=\frac{m_1\alpha_1+\cdots+m_r\alpha_r}{d}$

Proof: Write $\alpha=x_1\alpha_1+\cdots+x_r\alpha_r$ with $x_i\in\mathbb{Q}$. Let $\sigma_1,\dots,\sigma_r$ be the embeddings $\sigma_i: K/\mathbb{Q}\hookrightarrow\overline{\mathbb{Q}}$. We have

$\sigma_i(\alpha)=x_1\sigma_i(\alpha_1)+\cdots+x_r\sigma_i(\alpha_r)$ and

$$\begin{pmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_1(\alpha_r)\\ \vdots&&\\ \sigma_r(\alpha_1)&\cdots&\sigma_r(\alpha_r)\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_r\end{pmatrix}=\begin{pmatrix}\sigma_1(\alpha)\\ \vdots\\ \sigma_r(\alpha)\end{pmatrix}$$

By Cramer's rule,

$$x_j=\frac{\det\begin{pmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_1(\alpha)&\cdots&\sigma_1(\alpha_r)\\ &&\vdots\ (j)&&\\ \sigma_r(\alpha_1)&\cdots&\sigma_r(\alpha)&\cdots&\sigma_r(\alpha_r)\end{pmatrix}}{\det(\sigma_i(\alpha_j))=\delta}=\gamma_j$$

We have $\gamma_j\in\overline{\mathbb{Z}}$, since $\alpha,\alpha_i\in\mathcal{O}_K$. Also $\delta\in\overline{\mathbb{Z}}$. Notice that $\delta^2=d$ and $\delta x_j=\gamma_j \Rightarrow dx_j=\delta\gamma_j\in\overline{\mathbb{Z}}$. We also have $dx_j\in\mathbb{Q}$ and therefore, $dx_j\in\mathbb{Z}$, say $dx_j=m_j=\delta\gamma_j$. Then, $m_j^2=d\gamma_j^2$ and $\frac{m_j^2}{d}=\gamma_j^2\in\overline{\mathbb{Z}}$ since $\frac{m_j^2}{d}\in\mathbb{Q}$, we get $\frac{m_j^2}{d}\in\mathbb{Z} \Rightarrow d\mid m_j^2$ ∎

Coro: We have that $\mathcal{O}_K\subseteq\frac{\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_r}{d}$ and $\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_r\subseteq\mathcal{O}_K$

This implies that $\mathcal{O}_K$ is a free abelian group of rank r

$\mathcal{O}_K$ HAS A BASIS OVER $\mathbb{Z}$, SAY $\{\beta_1,\dots,\beta_r\}$ SUCH THAT $\mathcal{O}_K=\{l_1\beta_1+\dots+l_r\beta_r \mid l_i\in\mathbb{Z}\}$ CALLED AN INTEGRAL BASIS.

EX $\mathcal{O}_{\mathbb{Q}(\sqrt{r})}$ WITH r $\square$-FREE HAS INTEGRAL BASIS $\begin{cases}\{1,\sqrt{r}\} & \text{IF } r\equiv 2,3 \pmod 4\\ \{1,\frac{1+\sqrt{r}}{2}\} & \text{IF } r\equiv 1 \pmod 4\end{cases}$

THM: IF $\{\beta_1,\dots,\beta_r\}$ AND $\{\gamma_1,\dots,\gamma_r\}$ ARE INTEGRAL BASIS FOR $\mathcal{O}_K$, THEN $\operatorname{disc}(\beta_1,\dots,\beta_r)=\operatorname{disc}(\gamma_1,\dots,\gamma_r)$

PROOF WE MUST HAVE $\begin{pmatrix}\beta_1\\ \vdots\\ \beta_r\end{pmatrix}=M\begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_r\end{pmatrix}$, WHERE $M\in\mathbb{Z}^{r\times r}$

NOW APPLY σ_j AND GET

$(\sigma_j(\beta_i))=M(\sigma_j(\gamma_i))$. TAKING DETERMINANTS AND SQUARES, $\operatorname{disc}(\beta_1,\dots,\beta_r)=(\det M)^2\operatorname{disc}(\gamma_1,\dots,\gamma_r)$ AND $\det M\in\mathbb{Z}\Rightarrow$ $\operatorname{disc}(\beta_1,\dots,\beta_r)\mid\operatorname{disc}(\gamma_1,\dots,\gamma_r)$ WITH THE SAME SIGN.

BY THE REVERSE ARGUMENT WE GET THE EQUALITY $\neq$

REM THE DISCRIMINANT OF AN INTEGRAL BASIS IS AN INVARIANT OF THE FIELD. WE WRITE $\operatorname{disc}(K)$

EX $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{r})})=\begin{cases}\operatorname{disc}(\sqrt{r})=4r & r\equiv 2,3 \pmod 4\\ \operatorname{disc}(\frac{1+\sqrt{r}}{2})=r & r\equiv 1 \pmod 4\end{cases}$

OBS LET $\alpha_1,\dots,\alpha_r\in\mathcal{O}_K$. THEN

$\operatorname{disc}(\alpha_1,\dots,\alpha_r)=\operatorname{disc}(K)\iff\{\alpha_1,\dots,\alpha_r\}$ INTEGRAL BASIS.

$\operatorname{disc}(\alpha_1,\dots,\alpha_r)$ SQUARE-FREE $\Rightarrow\{\alpha_1,\dots,\alpha_r\}$ INTEGRAL BASIS.

THM LET $\omega_p=e^{2\pi i/p}$, p ODD PRIME. THEN $\mathcal{O}_{\mathbb{Q}(\omega_p)}=\mathbb{Z}[\omega_p]$

PROOF: WE WILL SEE THAT $\mathcal{O}_{\mathbb{Q}(\omega_p)}=\mathbb{Z}[1-\omega_p]$. LET $\alpha\in\mathcal{O}_{\mathbb{Q}(\omega_p)}$

$\alpha=\frac{m_0+m_1(1-\omega_p)+\dots+m_{p-2}(1-\omega_p)^{p-2}}{d}$ AND $\operatorname{disc}(\omega_p)=\operatorname{disc}(1-\omega_p)=\pm p^{p-2}$

IF $\mathcal{O}_{\mathbb{Q}(\omega_p)}\neq\mathbb{Z}[1-\omega_p]$, THERE IS $\beta\in\mathcal{O}_{\mathbb{Q}(\omega_p)}$ SUCH THAT NOT ALL m_i ARE DIVISIBLE BY d.

IT FOLLOWS THAT THERE IS A $\beta\in\mathcal{O}_K$ SUCH THAT

$\beta=\frac{m_1'(1-\omega_p)+\dots+m_{p-2}'(1-\omega_p)^{p-2}}{p}$ WITH $p\nmid m_i'$, $m_j'\in\mathbb{Z}$

NOTICE THAT $(1-\omega_p)\cdots(1-\omega_p^{p-1})=p$ AND SINCE $(1-\omega_p)\mid(1-\omega_p^k)$, WE GET

$\frac{p}{(1-\omega_p)^{p-1}}\in\mathbb{Z}[\omega_p]\Rightarrow\frac{p}{(1-\omega_p)^{i+1}}\in\mathbb{Z}[\omega_p]\Rightarrow\frac{\beta p}{(1-\omega_p)^{i+1}}\in\mathcal{O}_{\mathbb{Q}(\omega_p)}$

BY SUBTRACTING TERMS BELONGING TO $\mathcal{O}_{\mathbb{Q}(\omega_p)}$, WE OBTAIN

(18) $\frac{m_i'}{(1-\omega_p)} \in \mathcal{O}_{\mathbb{Q}(\omega_p)}$. Thus, $N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(1-\omega_p) \mid N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(m_i')$, where $N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(1-\omega_p) = p$ and $N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(m_i') = m_i'^{\,p-1}$.

This gives a contradiction #

Algebraic Number Theory

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

M. Lazin

Obs The theorem is still true for any $r \in \mathbb{Z}_{>0}$, $\mathcal{O}_{\mathbb{Q}(\omega_r)} = \mathbb{Z}[\omega_r]$

Def Consider two number number fields K, L. The **composite field** is $KL = \{a_1 b_1 + \dots + a_n b_n \mid a_i \in K, b_i \in L\}$ is the smallest field containing both K and L.

Clearly $\mathcal{O}_{KL} \supseteq \mathcal{O}_K \mathcal{O}_L = \{a_1 b_1 + \dots + a_n b_n \mid a_i \in \mathcal{O}_K, b_i \in \mathcal{O}_L\}$

When are they equal?

Let $d = (\operatorname{disc} \mathcal{O}_K, \operatorname{disc} \mathcal{O}_L)$, $r = [K:\mathbb{Q}]$, $s = [L:\mathbb{Q}]$

Thm Assume $[KL:\mathbb{Q}] = rs$. Then $\mathcal{O}_{KL} \subset \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$.

Coro If $[KL:\mathbb{Q}] = rs$ and $d = 1$, then $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$

Proof (Thm) Let $\{\alpha_1, \dots, \alpha_r\}$ and $\{\beta_1, \dots, \beta_s\}$ be basis for $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Then $\{\alpha_i \beta_j\}$ is an integral basis for $\mathcal{O}_K \mathcal{O}_L$ and a basis for KL. Let $\gamma \in \mathcal{O}_{KL}$. We can write

$$\gamma = \sum_{i,j} \frac{m_{ij}}{t} \alpha_i \beta_j,$$

where $m_{ij}, t \in \mathbb{Z}$, and there is no common factor

We need to show that $t \mid d$. It suffices to show that $t \mid \operatorname{disc}(\mathcal{O}_K)$ and apply symmetry. Consider $\sigma_1, \dots, \sigma_r \; K/\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$ with extensions $\sigma_1', \dots, \sigma_r' \; KL/L \hookrightarrow \overline{\mathbb{Q}}$. We have

$$\sigma'(\gamma) = \sum_{i,j} \frac{m_{ij}}{t} \sigma'(\alpha_i \beta_j) = \sum_{i,j} \frac{m_{ij}}{t} \sigma(\alpha_i) \beta_j$$

Set $x_i = \sum_{j=1}^{s} \frac{m_{ij}}{t} \beta_j$ then $\sum_{i=1}^{r} \sigma(\alpha_i) x_i = \sigma_j'(\gamma)$

By Cramer's rule,

$$x_j = \frac{\det \begin{pmatrix} \sigma_1(\alpha_1) \dots \sigma_1'(\gamma) \dots \sigma_1(\alpha_r) \\ \\ \sigma_r(\alpha_1) \dots \sigma_r'(\gamma) \dots \sigma_r(\alpha_r) \end{pmatrix}}{\det(\sigma_i(\alpha_j)) = \delta} = \frac{\gamma_j}{\delta}$$

$\gamma_j \in \mathbb{Z}$, since $\alpha_i, \gamma \in \mathcal{O}_{KL}$. Also $\delta \in \mathbb{Z}$. We know that $\delta^2 = \operatorname{disc}(\mathcal{O}_K) = e$. Since $\delta x_i = \gamma_i$, $e x_i = \delta \gamma_i \in \mathbb{Z}$

Now $e x_i = \sum_{j=1}^{} \frac{e m_{ij}}{t} \beta_j \in \mathbb{Z} \cap L = \mathcal{O}_L$. Since β_j is an integral basis for $\mathcal{O}_L$, and a basis for L, $\frac{e m_{ij}}{t} \in \mathbb{Z} \Rightarrow t \mid e m_{ij}$. Since t has no common factor with the m_{ij}, we get $t \mid e = \operatorname{disc}(\mathcal{O}_K)$ #.

Application Let $p \neq q$ be primes; then $\mathcal{O}_{\mathbb{Q}(\omega_{pq})} = \mathbb{Z}[\omega_{pq}]$

(The same can be proven in general.)

Algebraic Number Theory

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

M. Lazin

In the case of biquadratic fields, let $r, s \in \mathbb{Z}$, $(r,s) = 1$, $r \equiv s \equiv 1 \pmod 4$

Then $\mathcal{O}_{\mathbb{Q}(\sqrt{r}, \sqrt{s})} = \mathbb{Z}\left\{1, \frac{1+\sqrt{r}}{2}, \frac{1+\sqrt{s}}{2}, \frac{(1+\sqrt{r})(1+\sqrt{s})}{4}\right\}$

$\operatorname{disc} \mathbb{Q}(\sqrt{r}) = r$

$\operatorname{disc} \mathbb{Q}(\sqrt{s}) = s.$