Algebraic Number field or

Number field: An algebraic number field is a finite degree field extension of the field of rational numbers $\mathbb{Q}$. Here degree means the dimension of the field as a vector space over $\mathbb{Q}$.

Extension Field: A field K is said to be an extension field of a field F if F is a subfield of K. The notation is $K|F$ ie K is an extension field of F.

105

→ Field of Complex numbers is an extension field of field of real numbers $\mathbb{R}$.

→ $Q(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in Q \}$

$Q(\sqrt{2}) \mid Q$

$[Q(\sqrt{2}) : Q] = 2$

$\{1, \sqrt{2}\}$ forms a basis of $Q(\sqrt{2})$ as a vector space over Q.

→ $[\mathbb{C} : \mathbb{R}] = 2$, $B = \{1, i\}$

<u>Algebraic Element:</u> An element $a \in K$ is said to be algebraic over F if a is a root of a non-zero polynomial $f(x) \in F[x] = Q[x]$.

$\sqrt{2} \in Q(\sqrt{2})$ as $\sqrt{2}$ satisfies $x^2 - 2 \in F[x]$

Def: For a squarefree integer d other than 1, let

$$K = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

This is called quadratic ^number^ field as it has degree 2 over $\mathbb{Q}$.

Def: Let

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

This a subring of $\mathbb{Q}(\sqrt{d})$.

Note: 1. We will define the concept of "integers" for K which will play the same role in K as the ordinary integers $\mathbb{Z}$ do in $\mathbb{Q}$.

107

2. The integers of K will contain $\mathbb{Z}[\sqrt{d}]$ but may be larger.

3. Unique Factorization in the integers of K does not always hold.

4. In addition to the basic field operations, a quadratic field has an additional operation of Conjugation.

For $\alpha = x + y\sqrt{d} \in K$

$$\bar{\alpha} = x - y\sqrt{d}$$

(108)

Conjugation has the following properties.

1. $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$

2. $\overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}$

3. $\bar{\bar{\alpha}} = \alpha$

4. $\bar{\alpha} = \alpha \iff \alpha \in Q$

5. For any $\alpha \in K$, $\alpha + \bar{\alpha}$, $\alpha\bar{\alpha}$ are rational.

$\alpha + \bar{\alpha} = 2x$

$\alpha \cdot \bar{\alpha} = x^2 - dy^2$, $\alpha = x + y\sqrt{d}$

(109)

Def: (Trace): For $\alpha \in K$,

$$\alpha = x + y\sqrt{d} \in Q[\sqrt{d}],$$

$$x, y \in Q$$

$$Tr(\alpha) = \alpha + \bar{\alpha} = 2x$$

Norm of $\alpha = N(\alpha)$

$$= \alpha \bar{\alpha}$$

$$= x^2 - dy^2$$

<u>Note:</u> 1. $Tr(q) = 2q \quad ; q \in Q$

$$N(q) = q^2$$

2. Every $\alpha \in K = Q[\sqrt{d}]$ is a root of monic polynomial of degree 2 with rational coefficients.

110

$$(x-\alpha)(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$$

$$= x^2 - Tr(\alpha)x + N(\alpha)$$

Coefficients are Trace and Norm, might not be $\mathbb{Z}$,

if $\alpha = \frac{1}{2}$,

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - x + \frac{1}{4}$$

111

Integers in a Quadratic field

<u>Def:</u> An element $\alpha \in K = \mathbb{Q}[\sqrt{d}]$ is called an integer of K if the polynomial $x^2 - Tr(\alpha)x + N(\alpha)$ has coefficients in $\mathbb{Z}$, i.e, if $Tr(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$.

Exc: If $\alpha \in \mathbb{Z}[\sqrt{d}]$, then α is an integer of K.

Exc: If $d \equiv 1 \pmod 4$, then

$\frac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$, but it is an integer of $\mathbb{Q}(\sqrt{d})$ since $x^2 - x + \frac{1-d}{4}$ has coefficient in $\mathbb{Z}$.