

# Number Fields

Ömer Küçüksakallı

Middle East Technical University



September 1, 2016  
ECC 2016 – Summer School

1 Algebraic numbers

2 Algebraic integers

This lecture is based on the textbooks:

- Stewart, Tall - Algebraic Number Theory and Fermat's Last Theorem
- Marcus - Number Fields

# Algebraic numbers

## Definition

A complex number  $\alpha$  is called an algebraic number if it satisfies a non-zero polynomial equation with coefficients in  $\mathbf{Q}$ .

- Equivalently (clearing out denominators) we may assume the coefficients to be in  $\mathbf{Z}$ .

## Example

The roots of  $\frac{1}{2}x^2 - \frac{1}{3}x - \frac{1}{5} = 0$  are  $\frac{1}{3} \pm \sqrt{\frac{23}{45}}$ . These algebraic numbers are roots of the equation  $15x^2 - 10x - 6 = 0$  as well.

- The real numbers  $\pi$  and  $e = \exp(1)$  are not algebraic numbers. (A number which is not algebraic is called a transcendental number.)

# Algebraic numbers as a subfield of complex numbers

## Theorem

*The set of algebraic numbers is a subfield of  $\mathbf{C}$ .*

## Proof.

Recall that  $\alpha$  is an algebraic number if and only if  $[\mathbf{Q}(\alpha) : \mathbf{Q}]$  is finite. Suppose that  $\alpha, \beta$  are algebraic. The degree of a field extension is multiplicative in towers. Thus

$$[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}] = \underbrace{[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}(\alpha)]}_{\text{finite}} \underbrace{[\mathbf{Q}(\alpha) : \mathbf{Q}]}_{\text{finite}}.$$

It follows that  $\alpha \pm \beta, \alpha\beta$  and  $\alpha/\beta$  are algebraic numbers because they belong to  $\mathbf{Q}(\alpha, \beta)$ . □

- This proof is not constructive because it does not say anything about the minimal polynomials of the algebraic numbers  $\alpha + \beta$  and  $\alpha\beta$ .

# Computation of a minimal polynomial

- Suppose that we have two algebraic numbers  $\alpha$  and  $\beta$  which satisfy the polynomials equations  $3x^2 + 5x + 1 = 0$  and  $4x^3 - 5 = 0$ , respectively.
- How to find a polynomial  $P(x) \in \mathbf{Z}[x]$  so that  $P(\alpha + \beta) = 0$ ?
- Use Pari/GP.

```
? alpha=polroots(3*x^2+5*x+1)[1]
%1 = -1.4342585459106648821865368779117493244 + 0.E-38*I
? beta=polroots(4*x^3-5)[1]
%2 = 1.0772173450159418608796467832596752476 + 0.E-38*I
? algdep(alpha+beta,6)
%3 = 432*x^6 + 2160*x^5 + 4032*x^4 + 2360*x^3 - 1356*x^2 - 3180*x - 909
? algdep(alpha*beta,6)
%4 = 432*x^6 + 1600*x^3 + 25
? █
```

- Note that this method may not give the correct polynomial.

```
? polroots(x^3+123456789*x+111222333444555)[1]
%1 = -47235.397144436265819153816263379678756 + 0.E-38*I
? algdep(%,3)
%2 = 890436*x^3 + 42059452473*x^2 - 30495363367*x + 32709800546
? █
```

# Monomorphisms

- If  $K = \mathbf{Q}(\alpha)$  is a number field, then there are several distinct monomorphisms (one-to-one homomorphisms)  $\sigma : K \rightarrow \mathbf{C}$ .

## Example

If  $K = \mathbf{Q}(i)$  where  $i = \sqrt{-1}$ , then we have two possibilities. Namely  $\sigma_1(x + iy) = x + iy$  or  $\sigma_2(x + iy) = x - iy$  for  $x, y \in \mathbf{Q}$ .

- The full set of such monomorphisms plays an important role in algebraic number theory.

## Theorem

*Let  $K = \mathbf{Q}(\alpha)$  and let  $n = [K : \mathbf{Q}]$ . Then there are exactly  $n$  distinct monomorphisms  $\sigma_i : K \rightarrow \mathbf{C}$  where  $i = 1, \dots, n$ . The elements  $\sigma_i(\alpha)$  are the distinct zeros of the minimal polynomial of  $\alpha$  over  $\mathbf{Q}$ .*

## Definition

If  $\alpha$  is an algebraic number and  $K = \mathbf{Q}(\alpha)$  then the complex numbers  $\sigma_i(\alpha)$  are called the  $K$ -conjugates of  $\alpha$ .

- We have found that the element  $\gamma = \alpha + \beta$ , where  $3\alpha^2 + 5\alpha + 1 = 0$  and  $4\beta^3 - 5 = 0$ , is a root of the following polynomial equation:

$$432x^6 + 2160x^5 + 4032x^4 + 2360x^3 - 1356x^2 - 3180x - 909 = 0.$$

- Alternatively we can find it as follows:

```
? alpha=polroots(3*x^2+5*x+1);
? beta=polroots(4*x^3-5);
? 432*prod(i=1,2,prod(j=1,3,x-(alpha[i]+beta[j])))
%3 = 432*x^6 + (2160.000000000000000000000000000000 + 0.E-36*I)*x^5 + (4032.
000000000000000000000000000000000000 + 0.E-35*I)*x^4 + (2360.00000000000000000000
00000000000000 + 0.E-35*I)*x^3 + (-1356.0000000000000000000000000000000000 + 0.E-
35*I)*x^2 + (-3180.0000000000000000000000000000000000 + 0.E-35*I)*x + (-909.0000
00000000000000000000000000000001 + 0.E-36*I)
? round(%)
%4 = 432*x^6 + 2160*x^5 + 4032*x^4 + 2360*x^3 - 1356*x^2 - 3180*x - 909
? █
```



# Discriminants

- Let  $K = \mathbf{Q}(\alpha)$  and let  $\{\alpha_1, \dots, \alpha_n\}$  be a basis of  $K$  as a vector space over  $\mathbf{Q}$ .

## Definition

The discriminant of this basis is defined to be

$$\text{disc}(\alpha_1, \dots, \alpha_n) = (\det[\sigma_i(\alpha_j)])^2.$$

- If we pick another basis  $\{\beta_1, \dots, \beta_n\}$ , then

$$\beta_k = \sum_{i=1}^n c_{ik} \alpha_i, \quad \text{where } c_{ik} \in \mathbf{Q}.$$

- The product formula for determinants and the fact that  $\sigma_i$  are monomorphisms shows that

$$\text{disc}(\beta_1, \dots, \beta_n) = \det([c_{ik}])^2 \text{disc}(\alpha_1, \dots, \alpha_n).$$

# The discriminant is non-zero

## Theorem

*The discriminant of any basis for  $K = \mathbf{Q}(\alpha)$  is rational and non-zero.*

## Proof.

Pick a basis  $\{1, \alpha, \dots, \alpha^{n-1}\}$ . The general result would follow because the change of basis matrix has rational entries and nonzero determinant. If the conjugates of  $\alpha$  are  $\alpha_1, \dots, \alpha_n$ , then

$$\text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \left( \det[\alpha_i^j] \right)^2 = \left( \prod_{1 \leq i, j \leq n} (\alpha_i - \alpha_j) \right)^2.$$

The second equality follows from the Vandermonde determinant. □

# Polynomial discriminant

- Let  $K = \mathbf{Q}(\alpha)$  be a number field. The polynomial discriminant of  $\min_{\alpha, \mathbf{Q}}$  and the discriminant  $\text{disc}(1, \alpha, \dots, \alpha^{n-1})$  are the same.
- Consider a quadratic polynomial  $ax^2 + bx + c \in \mathbf{Q}[x]$  with roots  $x_1, x_2$ . Note that  $x_1 + x_2 = \frac{-b}{a}$  and  $x_1x_2 = \frac{c}{a}$ . We have

$$\begin{aligned} \left( \prod_{1 \leq i, j \leq 2} (x_i - x_j) \right)^2 &= (x_1 - x_2)^2 \\ &= (x_1 + x_2)^2 - 4x_1x_2 \\ &= \left( \frac{-b}{a} \right)^2 - 4 \frac{c}{a} \\ &= \frac{b^2 - 4ac}{a^2}. \end{aligned}$$

# Algebraic integers

## Definition

A complex number  $\alpha$  is called an algebraic integer if there is a **monic** polynomial  $P(x)$  with integer coefficients such that  $P(\alpha) = 0$ .

- Any integer  $n \in \mathbf{Z}$  is an algebraic integer because it is a root of  $x - n = 0$ .
- There are obvious algebraic integers such as  $\sqrt[m]{n}$ . They are the roots of  $x^m - n = 0$
- There are less obvious algebraic integers such as
  - $\frac{\sqrt{5} + 1}{2}$  which is a root of  $x^2 + x - 1 = 0$ . (Golden ratio)
  - $\frac{\sqrt[3]{19}^2 + \sqrt[3]{19} + 1}{3}$  which is a root of  $x^3 - x^2 - 6x - 12 = 0$ .

# Minimal polynomial of an algebraic integer

- Notice that we have not required that the polynomial  $P(x)$  be irreducible over  $\mathbf{Q}$ .
- In this way, we can easily see that  $\zeta_m = \exp(2\pi i/m)$  is an algebraic integer.

## Theorem

*If  $\alpha$  is an algebraic integer then  $\min_{\alpha, \mathbf{Q}} \in \mathbf{Z}[x]$ .*

- In other words, the monic irreducible polynomial over  $\mathbf{Q}$  having  $\alpha$  as a root has coefficients in  $\mathbf{Z}$ . This can be proved by the following lemma.

## Lemma

*Let  $f$  be a monic polynomial with coefficients in  $\mathbf{Z}$ , and suppose  $f = gh$  where  $g$  and  $h$  are monic polynomials with coefficients in  $\mathbf{Q}$ . Then  $g$  and  $h$  actually have coefficients in  $\mathbf{Z}$ .*

# Number fields of degree one and two

- The only algebraic integers in  $\mathbf{Q}$  are the ordinary integers because

$$\min_{\alpha \in \mathbf{Q}} |x - \alpha| = x - r \in \mathbf{Z}[x].$$

- Let  $K/\mathbf{Q}$  be a quadratic extension. Then there exists a squarefree integer  $m$  such that  $K = \mathbf{Q}(\sqrt{m})$ .
- The set of algebraic integers in the quadratic field  $\mathbf{Q}(\sqrt{m})$  is
  - $\{a + b\sqrt{m} : a, b \in \mathbf{Z}\}$  if  $m \equiv 2, 3 \pmod{4}$ ,
  - $\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbf{Z}, a \equiv b \pmod{2}\}$  if  $m \equiv 1 \pmod{4}$ .
- Note that in each case we obtain a subring of the number field  $K$ .
- In order to prove this, we need a lemma first.

# Equivalent conditions for being an algebraic integer

## Lemma

The following are equivalent for  $\alpha \in \mathbf{C}$ .

- 1  $\alpha$  is an algebraic integer;
- 2 The additive group of the ring  $\mathbf{Z}[\alpha]$  is finitely generated;
- 3  $\alpha$  is a member of some subring of  $\mathbf{C}$  having a finitely generated additive group;
- 4  $\alpha A \subset A$  for some finitely generated additive subgroup  $A \subset \mathbf{C}$ .

## Proof.

The implications (1)  $\implies$  (2)  $\implies$  (3)  $\implies$  (4) are relatively easier to see. For the implication (4)  $\implies$  (1), use the determinant procedure.  $\square$

- We explain the determinant procedure with an example.



# Determinant procedure with an example

- Consider algebraic integers  $\alpha$  and  $\beta$  with  $\alpha^2 + \alpha + 1 = 0$  and  $\beta^3 - 5 = 0$ . Consider a basis of  $\mathbf{Q}(\alpha, \beta)$  over  $\mathbf{Q}$ .

$$\left\{ \underbrace{1}_{x_1}, \underbrace{\alpha}_{x_2}, \underbrace{\beta}_{x_3}, \underbrace{\beta\alpha}_{x_4}, \underbrace{\beta^2}_{x_5}, \underbrace{\beta^2\alpha}_{x_6} \right\}.$$

- Use  $\alpha^2 = -\alpha - 1$  and  $\beta^3 = 5$  whenever it is necessary.

$$(\alpha + \beta)x_1 = x_2 + x_3,$$

$$(\alpha + \beta)x_2 = -x_1 - x_2 + x_4,$$

$$(\alpha + \beta)x_3 = x_4 + x_5,$$

$$(\alpha + \beta)x_4 = -x_3 - x_4 + x_6,$$

$$(\alpha + \beta)x_5 = 5x_1 + x_6,$$

$$(\alpha + \beta)x_6 = 5x_2 - x_5 - x_6.$$

# Determinant procedure with an example

- The element  $\alpha + \beta$  can be realized as an eigenvalue of a  $6 \times 6$  matrix.

$$(\alpha + \beta) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 & 1 \\ 5 & 0 & 0 & 0 & 0 & 1 \\ 0 & 5 & 0 & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

- We can abbreviate this equation by  $(\alpha + \beta)\mathbf{x} = M\mathbf{x}$ . The characteristic polynomial of  $M$  is

$$\det(xI - M) = x^6 + 3x^5 + 6x^4 - 3x^3 - 9x^2 + 18x + 36$$

- This polynomial has  $\alpha + \beta$  as a root because it is an eigenvalue of  $M$ .

# Algebraic integers as a subring of complex numbers

## Theorem

*The algebraic integers form a subring of the field of algebraic numbers.*

## Proof.

A complex number  $\alpha$  is an algebraic integer if and only if  $\mathbf{Z}[\alpha]$  is finitely generated. Let  $\alpha$  and  $\beta$  be two algebraic integers. Suppose that  $\mathbf{Z}[\alpha]$  is generated by  $\alpha_1, \dots, \alpha_m$  and  $\mathbf{Z}[\beta]$  is generated by  $\beta_1, \dots, \beta_n$ . Then  $\mathbf{Z}[\alpha, \beta]$  is finitely generated by the  $mn$  products  $\alpha_i\beta_j$ . Finally,  $\mathbf{Z}[\alpha, \beta]$  contains  $\alpha + \beta$  and  $\alpha\beta$ . By characterization (3), this implies that they are algebraic integers.  $\square$

## Definition

Let  $\mathbf{A}$  be the subring of  $\mathbf{C}$  which contain all algebraic integers. For any number field  $K$ , we write

$$\mathcal{O}_K = K \cap \mathbf{A},$$

and call  $\mathcal{O}_K$  the ring of integers of  $K$ .

- Both  $K$  and  $\mathbf{A}$  are subrings of  $\mathbf{C}$ . Thus  $\mathcal{O}_K$  is a subring too.
- If  $\alpha \in K$  then for some non-zero  $c \in \mathbf{Z}$  we have  $c\alpha \in \mathcal{O}_K$ .
- If  $K$  is a number field then  $K = \mathbf{Q}(\alpha)$  for some algebraic integer  $\alpha$ .

- The ring  $\mathcal{O}_K$  of integers of  $K$  is an abelian group under addition.
- A  $\mathbf{Z}$ -basis for  $(\mathcal{O}_K, +)$  is called an integral basis for  $\mathcal{O}_K$  (or for  $K$ ).

## Theorem

*Every number field  $K$  admits an integral basis of rank  $n = [K : \mathbf{Q}]$ .*

- Integral bases are not always what naively we might expect them to be. Consider the following examples:

$\alpha^2 + 1 = 0$	$\alpha^2 + 3 = 0$	$\alpha^3 - 2 = 0$	$\alpha^3 - 19 = 0$
$\{1, \alpha\}$	$\{1, (1 + \alpha)/2\}$	$\{1, \alpha, \alpha^2\}$	$\{1, \alpha, (1 + \alpha + \alpha^2)/3\}$

# The discriminant of a number field

- If  $\{\alpha_1, \dots, \alpha_n\}$  is a basis of  $K$  consisting of algebraic integers, then the discriminant  $\text{disc}(\alpha_1, \dots, \alpha_n)$  is an ordinary integer, not equal to zero.
- For two integral bases  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta_1, \dots, \beta_n\}$  of  $K$ , we have

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \text{disc}(\beta_1, \dots, \beta_n)$$

- To see this, note that change of base matrix is unimodular and it has determinant  $\pm 1$ . Also recall that discriminant involves squaring.

## Definition

If  $\{\alpha_1, \dots, \alpha_n\}$  is an integral basis for  $K$ , then the integer  $\text{disc}(\alpha_1, \dots, \alpha_n)$  is called the discriminant of  $K$ , denoted  $d_K$ .

# The discriminant of a subgroup

- If we can find a maximal set of algebraic integers linearly independent over  $\mathbf{Q}$ , then they generate a subgroup of  $\mathcal{O}_K$  of finite index.
- More precisely we have the following:

## Theorem

*Let  $G$  be an additive subgroup of  $\mathcal{O}_K$  of rank equal to the degree of  $K$ , with  $\mathbf{Z}$ -basis  $\{\alpha_1, \dots, \alpha_n\}$ . Then  $|\mathcal{O}_K/G|^2$  divides  $\text{disc}(\alpha_1, \dots, \alpha_n)$ .*

- This theorem has a useful consequence in finding integral bases for some number fields.

## Corollary

*Suppose  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$  form a  $\mathbf{Q}$ -basis for  $K$ . If  $\text{disc}(\alpha_1, \dots, \alpha_n)$  is squarefree then  $\{\alpha_1, \dots, \alpha_n\}$  is an integral basis.*

## Example

- Consider the number field  $K = \mathbf{Q}(\alpha)$  where  $\alpha^3 - \alpha - 1 = 0$ .
- The basis  $\{1, \alpha, \alpha^2\}$  for  $K$  over  $\mathbf{Q}$  consist of algebraic integers. Thus it generates a subgroup of  $\mathcal{O}_K$  of finite index.
- We compute that

$$\text{disc}(1, \alpha, \alpha^2) = \det \left( \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \sigma(\alpha) & \sigma(\alpha^2) \\ 1 & \tau(\alpha) & \tau(\alpha^2) \end{bmatrix} \right)^2 = -23.$$

- The previous corollary implies that  $\{1, \alpha, \alpha^2\}$  is an integral basis.
- The discriminant of the number field is  $d_K = -23$ .



- The converse of this criteria is not correct. There are plenty of number fields whose discriminant is not square-free.

## Example

- Consider  $K = \mathbf{Q}(\sqrt{-1})$ , then we have

$$\text{disc}(1, \sqrt{-1}) = \det \left( \begin{bmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{bmatrix} \right)^2 = -4.$$

- Let  $G$  be the free abelian group generated by the basis  $\{1, \sqrt{-1}\}$ . In order to show that  $\mathcal{O}_K = G$ , we need to see that  $[\mathcal{O}_K/G] \neq 2$ .
- The element  $\alpha = \frac{a+b\sqrt{-1}}{2}$  has minimal polynomial

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - ax + \frac{a^2 + b^2}{4}.$$

- Its coefficients can be integer only if both  $a$  and  $b$  are even.

- Norm and trace often allow us to transform a problem about algebraic integers into one about the rational integers.
- Let  $K = \mathbf{Q}(\alpha)$  be a number field and  $\sigma_i : K \rightarrow \mathbf{C}$  be its distinct monomorphisms into  $\mathbf{C}$ .
- For any  $\alpha \in K$ , we define the norm

$$N_K(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$$

- and the trace

$$T_K(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

# A discriminant formula by the norm

- Discriminants involve complicated work with determinants. Thus the following result is sometimes useful.

## Theorem

Let  $K = \mathbf{Q}(\alpha)$  be a number field where  $\alpha$  has a minimal polynomial  $P(x)$  of degree  $n$ . Let  $P'(x)$  be the formal derivative of  $P(x)$ . The  $\mathbf{Q}$ -basis  $\{1, \alpha, \dots, \alpha^{n-1}\}$  has discriminant

$$\text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \pm N_K(P'(\alpha))$$

where the plus sign holds if and only if  $n \equiv 0, 1 \pmod{4}$ .

# An application of the norm map

- Let  $\alpha$  be a root of the irreducible polynomial  $f(x) = x^3 + ax + b$  with integer coefficients.
- We have  $f'(\alpha) = 3\alpha^2 + a = -\frac{2a\alpha+3b}{\alpha}$ .
- It is easy to see that  $2a\alpha + 3b$  is a root of

$$\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b = 0$$

Using this we find that  $N(2a\alpha + 3b) = 27b^3 + 4a^3b$ .

- On the other hand  $N(\alpha) = -b$ .
- The previous theorem implies that

$$\text{disc}(1, \alpha, \alpha^2) = N(f'(\alpha)) = -(4a^3 + 27b^2).$$

## Example

Let us find the ring of integers of  $\mathbf{Q}(\alpha)$  where  $\alpha = \sqrt[3]{5}$ .

- Our first natural guess is  $\mathcal{O}_K$  has  $\mathbf{Z}$ -basis  $\{1, \alpha, \alpha^2\}$ .
- We have  $\text{disc}(1, \alpha, \alpha^2) = -3^3 5^2$ .
- We must consider two possibilities
  - ① Can  $\beta = \frac{1}{3} (\lambda_1 + \lambda_2 \alpha + \lambda_3 \alpha^2)$  be an algebraic integer, for  $0 \leq \lambda_i \leq 2$ ?
  - ② Can  $\gamma = \frac{1}{5} (\lambda_1 + \lambda_2 \alpha + \lambda_3 \alpha^2)$  be an algebraic integer, for  $0 \leq \lambda_i \leq 4$ ?
- We first make an extensive search and eliminate the first possibility.

# Continue

```
? pr=polroots(x^3-5);
? for(i=0,2,for(j=0,2,for(k=0,2,print([i,j,k,round(prod(l=1,3,x-(i+j*pr[l]+k*pr[l]^2)))]))))
[0, 0, 0, x^3]
[0, 0, 1, x^3 - 25]
[0, 0, 2, x^3 - 200]
[0, 1, 0, x^3 - 5]
[0, 1, 1, x^3 - 15*x - 30]
[0, 1, 2, x^3 - 30*x - 205]
[0, 2, 0, x^3 - 40]
[0, 2, 1, x^3 - 30*x - 65]
[0, 2, 2, x^3 - 60*x - 240]
[1, 0, 0, x^3 - 3*x^2 + 3*x - 1]
[1, 0, 1, x^3 - 3*x^2 + 3*x - 26]
[1, 0, 2, x^3 - 3*x^2 + 3*x - 201]
[1, 1, 0, x^3 - 3*x^2 + 3*x - 6]
[1, 1, 1, x^3 - 3*x^2 - 12*x - 16]
[1, 1, 2, x^3 - 3*x^2 - 27*x - 176]
[1, 2, 0, x^3 - 3*x^2 + 3*x - 41]
[1, 2, 1, x^3 - 3*x^2 - 27*x - 36]
[1, 2, 2, x^3 - 3*x^2 - 57*x - 181]
[2, 0, 0, x^3 - 6*x^2 + 12*x - 8]
[2, 0, 1, x^3 - 6*x^2 + 12*x - 33]
[2, 0, 2, x^3 - 6*x^2 + 12*x - 208]
[2, 1, 0, x^3 - 6*x^2 + 12*x - 13]
[2, 1, 1, x^3 - 6*x^2 - 3*x - 8]
[2, 1, 2, x^3 - 6*x^2 - 18*x - 153]
[2, 2, 0, x^3 - 6*x^2 + 12*x - 48]
[2, 2, 1, x^3 - 6*x^2 - 18*x - 13]
[2, 2, 2, x^3 - 6*x^2 - 48*x - 128]
?
```

- We must disprove:
  - Can  $\gamma = \frac{1}{5}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2)$  be an algebraic integer, for  $0 \leq \lambda_i \leq 4$ ?
- Assume  $\gamma \in \mathcal{O}_K$ . Then  $N(\gamma)$  and  $T(\gamma)$  are ordinary integers.
- Using the trace map, we see that  $T(\gamma) = \frac{3c_1}{5}$  which must be an integer. Thus  $c_1$  must be a multiple of 5. Without loss of generality

$$\gamma = \frac{1}{5}(\lambda_2\alpha + \lambda_3\alpha^2).$$

- In this case, we have  $N(\gamma) = \frac{5\lambda_2^3 + 25\lambda_3^3}{125}$  and it must be an integer.
- Assume that  $\lambda_2^3 + 5\lambda_3^3 \equiv 0 \pmod{25}$ .
- If  $\lambda_3 \equiv 0 \pmod{5}$ , then  $\lambda_2 \equiv 0 \pmod{5}$ .
- If not, we have  $(-\frac{\lambda_2}{\lambda_3})^3 \equiv 5 \pmod{25}$ , a contradiction.
- Thus we conclude that  $\mathcal{O}_{\mathbf{Q}(\sqrt[3]{5})} = \mathbf{Z}[\sqrt[3]{5}]$ .

# A power basis may not exist

- Consider the the number field  $K = \mathbf{Q}(\sqrt[3]{175})$ .
- We will show that there is no integral basis of the form  $\{1, \theta, \theta^2\}$ .
- Let  $t = \sqrt[3]{5^2 \cdot 7}$ . Consider also  $u = \sqrt[3]{5 \cdot 7^2}$ . It turns out that  $\{1, t, u\}$  is a basis for  $\mathcal{O}_K$  and  $\text{disc}(1, t, u) = -3^3 \cdot 5^2 \cdot 7^2$ .
- $\{1, \theta, \theta^2\}$  is a basis  $\Leftrightarrow \{1, \theta + 1, (\theta + 1)^2\}$  is a basis. Without loss of generality we can assume that  $\theta = (bt + cu)$ .
- We have  $(bt + cu)^2 = 70bc + 7c^2t + 5b^2u$ . A change of bases matrix between  $\{1, t, u\}$  and  $\{1, \theta, \theta^2\}$  is given by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{bmatrix}$$

- The assumption that this matrix has determinant  $5b^3 - 7c^3 = \pm 1$  implies that  $5b^3 \equiv \pm 1 \pmod{7}$ , a contradiction.



# Integral basis for compositum

## Theorem

Let  $K$  and  $L$  be number fields with  $K \cap L = \mathbf{Q}$ . If  $d = \gcd(d_K, d_L)$  then

$$\mathcal{O}_{KL} \subset \frac{1}{d} \mathcal{O}_K \mathcal{O}_L.$$

- Note that the inclusion  $\mathcal{O}_{KL} \supset \mathcal{O}_K \mathcal{O}_L$  is trivially true.

## Example

- Consider  $K = \mathbf{Q}(\sqrt{5})$  with an integral basis  $\{1, \alpha\}$  where  $\alpha = (\sqrt{5} + 1)/2$ . Consider also  $L = \mathbf{Q}(\sqrt{-1})$  with an integral basis  $\{1, \beta\}$  where  $\beta = \sqrt{-1}$ .
- Note that  $d_K = 5$  and  $d_L = -4$  which are relatively prime.
- Thus  $\{1, \alpha, \beta, \alpha\beta\}$  is an integral basis for  $\mathbf{Q}(\sqrt{5}, \sqrt{-1})$ .

## Example

- Consider  $K = \mathbf{Q}(\sqrt{2})$  with an integral basis  $\{1, \alpha\}$  where  $\alpha = \sqrt{2}$ . Consider also  $K = \mathbf{Q}(\sqrt{-1})$  with an integral basis  $\{1, \beta\}$  where  $\beta = \sqrt{-1}$ .
- Note that  $d_K = 8$  and  $d_L = -4$  which are **not** relatively prime.
- The previous theorem implies that

$$\mathcal{O}_{KL} \subset \frac{1}{4}\mathcal{O}_K\mathcal{O}_L.$$

- Indeed the element  $\zeta = \frac{\sqrt{2} + \sqrt{-2}}{2} \in KL$  is an algebraic integer. To see this, we note that  $\zeta = \exp(2\pi i/8)$  and  $\zeta^8 - 1 = 0$ .
- An integral basis for  $\mathbf{Q}(\sqrt{2}, \sqrt{-1})$  is  $\{1, \zeta, \zeta^2, \zeta^3\}$ .
- In general  $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$  where  $\zeta_n = \exp(2\pi i/n)$ .

# A useful form of the integral basis

## Theorem

Let  $\alpha \in \mathcal{O}_K$  and suppose  $\alpha$  has degree  $n$  over  $\mathbf{Q}$ . Then there is an integral basis

$$\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}} \right\}$$

where the  $d_i$  are in  $\mathbf{Z}$  and satisfy  $d_1 | d_2 | \dots | d_{n-1}$ ;  $f_i$  are monic polynomials over  $\mathbf{Z}$ , and  $f_i$  has degree  $i$ . The  $d_i$  are uniquely determined.

## Example

- Consider the number field  $\mathbf{Q}(\alpha)$  with  $\alpha = \sqrt[3]{28}$ . An integral basis for this number field, in the above form, is given by

$$\left\{ 1, \theta, \frac{\theta^2 + 4\theta + 4}{6} \right\}$$

# The End