Algebraic Number Theory
3704

Dr H Wilton

Jan 2012

Contents

1 Introduction

An Algebraic number is the root of a polynomial.
eg. $\alpha = \sqrt{2},\ 15\sqrt[7]{3},\ 2+i, \ldots$ such that $f(\alpha) = 0$ where $f \in \mathbb{Z}[x]$ or $\mathbb{Q}[x]$
An Algebraic number field
$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{2}$
also $\mathbb{Q}(i + \sqrt{2})$ for example
K is an algebraic number field $\underbrace{\sigma}_{\text{algebraic integers}} \subseteq K$ eg. $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$
Typical questions to ask about σ

(i) Does σ have unique factorisation?

(ii) Is σ a PID?

(iii) If not then how close is σ to being a PID?

(iv) How does a prime p factorise in σ?
eg. in $\mathbb{Z}[i]$, $5 = (\sqrt{2}+1)(\sqrt{2}-1)$ but 7 doesn't factorise.

(v) What are the units of σ?
eg. $(\sqrt{2}+1)(\sqrt{2}-1) = 1$ in $\mathbb{Z}(\sqrt{2})$ but in $\mathbb{Z}(\sqrt{-5})$ only $1, -1$ are units.

2 Fields

2.1 Background material

Rings - commutative with 1
K - a field
Rings of interest

1. $\mathbb{Z}$

2. $K[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i \mid a^i \in K\}$

Members of the ring:

(i) units - irreducible elements

(ii) reductible elements $f = gh,\ g, h$ non units

(iii) irreductible elements, everything else

eg. Units of $K[x] = K^*$

Criteria for irreductibility of $f \in \mathbb{Q}[x]$

(i) Gauss lemma: If f is irreducible in $\mathbb{Z}[x]$ then f is irreducible in $\mathbb{Q}[x]$
Corollary: if f is monic of degree 2 or 3 then if f is reductible it has a root in $\mathbb{Z}$ which has to divide the constant term of f. eg. $x^3 + x + 1$

(ii) Eissenstein Criterion: $f(x) = \sum_{i=0}^{n} a_i x^i$ if there is p a prime such that:

  (a) $p \mid a_i, \ i < n$

  (b) $p \nmid a_n$

  (c) $p \nmid a_0$

  then f is irreducible. eg. for: $x^2 + 4x + 2$

(iii) Reduction mod p
  if $f \in \mathbb{Z}[x]$ denote the map:

$$\mathbb{Z}[x] \to (\mathbb{Z}/p)[x]$$
$$by \quad f \to f$$

  if the degree of the polynomial doesn't go down and deg f = deg f and f is irreductible in $(\mathbb{Z}/p)[x]$, then f is irreductible in $\mathbb{Z}[x]$.

Also note that $\underbrace{f(x)}_{\in\mathbb{Z}[x]}$ s irreductable iff $f(x+a)$ is irreductable where $a \in \mathbb{Z}$

Definition 2.1 (Euclid's algorithm)**.** *If $f, g \in K[x]$ then we can write*

$$f(x) = h(x)g(x) + r(x) \qquad deg(r) < deg(g)$$

$$hcf(f, g) = hcf(g, r) = \dots$$

Definition 2.2. *A ring with a euclidean algorithm is called a euclidean domain eg. $\mathbb{Z}[x],\ K[x]$ where a euclidean algorithm assigns each menber of the ring a degree $deg : R \to \mathbb{N}$*

Definition 2.3 (Ideal)**.** *R-ring, $I \subseteq R,\ I \neq \phi$ is called an ideal if:*

(i) $x, y \in I \Rightarrow x + y \in I$

(ii) $x \in I,\ \lambda \in R \Rightarrow \lambda x \in I$

$$eg.\ x \in R \ then\ (x) = \{\lambda x \mid \lambda \in R\} \ - \ Principal\ ideal.$$

$$Also\ (x_1, \dots, x_n) = \left\{ \sum_{i=1}^{n} \lambda_i x^i \mid \lambda_i \in R \right\} \ eg.\ \underbrace{(4,6)}_{\subset\mathbb{Z}} = (hcf(4,6)) = (2)$$

Definition 2.4. *If every ideal in R is a principal ideal then R is a principal ideal domain.*

Theorem 2.1 (Euclidean rings are PID)**.**

Proof. $I \subseteq R$, ideal. Take $x \in I/0$ of minimal degree. Let $y \in I$ then

$$y = gx + r, \quad deg(r) < deg(x), \quad r \in I \quad \Rightarrow r = 0$$

$\square$

Definition 2.5 (Maximal ideal). *an ideal $I \subseteq R$ is maximal if for any ideal J with $I \subseteq J \subseteq R$ either $I = J$ or $J = R$.*

Example 2.1. *maximal ideals in $K[x]$ are all of the form (f) where f is and irreductable polynomial. for (g) if $g = hk$ then $(g) \subsetneq (h)$.*

Definition 2.6. *Let $I \subseteq R$ be an ideal then $(I, +) \subseteq (R, +)$ is a subgroup. We can consider the group*

$$R/I = \{x + I \mid x \in R\}$$

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I)(y + I) = xy + I$$

R/I is the quotient of R by I.

Definition 2.7. *If R, S are rings, $\phi : R \to S$ is a ring homomorphism if:*

(i) $\phi(a + b) = \phi(a) + \phi(b)$

(ii) $\phi(ab) = \phi(a)\phi(b)$

(iii) $\phi(1) = 1$

Lemma 2.2. *If K is a field and $I \subseteq K$ is an ideal then $I = \{0\}$ or $I = \{K\}$*

Proof. If $x \in I/\{0\}$ and $y \in K$ be arbitrary. Then

$$\underbrace{(yx^{-1})x}_{=y} \in I$$

□

Corollary 2.1. *If $\phi : K \to R$ is a ring homomorphism where K is a field and R is a ring, then ϕ is injective.*

Proof.

$$\phi(1) = 1_R \text{ so } 1 \notin ker(\phi) \Rightarrow ker(\phi) \neq K \therefore ker(\phi) = \{0\}$$

□

Theorem 2.3. *An ideal $i \subset R$ is maximal iff R/I is a field.*

Proof.
($\Leftarrow$) Let

$$\phi : R \to R/I, \quad \phi : x \mapsto x + I \qquad \text{be the quotient homomorphism}$$

Suppose $I \subseteq J \subseteq R$ then

$$\phi(J) \subseteq R/I$$

is an ideal. By the lemma 2.2

$$\phi(J) = \{0\} \Rightarrow J = I$$
$$\phi(J) = R/I \Rightarrow J = R$$

($\Rightarrow$) Suppose $I \subseteq R$ is maximal and consider $x \in R/I$. We need to show that $x + I \in R/I$ has a multiplicative inverse. The ideal generated by x and I is R. $1 \in R$ so there is $y \in R$ and $\xi \in I$ such that

$$xy + \xi = 1 \Rightarrow 1 \in xy + I = (x + I)(y + I)$$

$x + I$ has a multiplicative inverse, hence R/I is a field. □

2.2 Field Extentions

Definition 2.8. *if K, L are fields and $K \subseteq L$ then K is a subfield of L and L is an extention of K*

Example 2.2.

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
$$K \subseteq L \subseteq \mathbb{C}$$

Definition 2.9. *An element $\alpha \in L$ is algebraic over K if:*

$$\exists f(x) \in K[x] \quad \text{such that} \quad f(\alpha) = 0.$$

Usually $k = \mathbb{Q}$

Definition 2.10. *The ring generated by K and $\alpha \in L$ is denoted $K[\alpha]$:*

$$K[\alpha] = \{f(\alpha) \mid f \in K[x]\}.$$

Definition 2.11. *The field generated by K and $\alpha \in L$ is denoted $K(\alpha)$:*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[x],\ g(\alpha) \neq 0 \right\}.$$

Definition 2.12.

$$I(\alpha) = \{f \in K[x] \mid f(\alpha) = 0\}.$$

Lemma 2.4. *$I(\alpha)$ is an ideal.*

Proof. $f, g \in I(\alpha)$

$$(f + g)(\alpha) = f(\alpha) + g(\alpha) = 0 + 0$$

$f \in I(\alpha),\ g \in K[x]$

$$(fg)(\alpha) = f(\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$$

□

Definition 2.13. *$K[x]$ is a PID*

$$I(\alpha) = (M)$$

M is well defined up to multiplication by $\lambda \in K^*$, because it's minimum degree element of $I(\alpha)$

Definition 2.14. *The minimal polynomial of α, M_α, is the unique monic polynomial such that*

$$I(\alpha) = M_\alpha$$

Example 2.3. $\alpha = \sqrt{2}, \quad k = \mathbb{Q}$

$$M_\alpha(x) = x^2 - 2$$

Lemma 2.5. *$I(x)$ is maximal or equlivlently, M_α is irreductable.*

Proof. suppose M_α is reductable then:

$$M_\alpha(x) = a(x)b(x)$$
$$M_\alpha(\alpha) = a(\alpha)b(\alpha) = 0$$

Without loss of generality

$$a(\alpha) = 0 \Rightarrow a \in I(\alpha) = (M_\alpha)$$

So $M_\alpha | a$ and $deg(a) = deg(M_\alpha)$ so $b(x)$ is constant. $b(x)$ is a unit in $K[x]$ and so M_α is irreductable. ☐

Lemma 2.6. *A polynomial M is the minimal polynomial of α if:*

(i) $M(\alpha) = 0$

(ii) M *is monic*

(iii) M *is irreductable*

Proof.
($\Rightarrow$) already done
($\Leftarrow$)

$$(i) \Rightarrow M \in I(\alpha) = (M_\alpha)$$
$$\Rightarrow M_\alpha | M \text{ } ie \text{ } M = a \cdot M_\alpha$$

by (iii) $a \in K^*$, compare coefficents and using the fact, (ii), that M is monic

$$x^m = ax^n \Rightarrow a = 1$$

☐

we just proved that proved that $I(\alpha)$ is a maximal ideal, so $K[x]/I(\alpha)$ is a field.

Theorem 2.7. *Let $\alpha \in L$ be algebraic over K. Then:*

$$\Phi : \quad k[x]/I(\alpha) \to k(\alpha)$$
$$f + (M_\alpha) \mapsto f(\alpha)$$

is a field isomorphism and $K[\alpha] = k(\alpha)$.

Proof. first we need to check Φ is well defined. Suppose:

$$g \in f + (M_\alpha) \Leftrightarrow [f - g \in (M_\alpha)]$$

then

$$\Phi(g + (M_\alpha)) = g(\alpha) = f(\alpha) = \Phi(f + (M_\alpha))$$

next we should check that Φ is a ring homomorphism.

$$\Phi(1 + (M_\alpha)) = 1$$

$$\Phi(f + g + (M_\alpha)) = f + g = \Phi(f + (M_\alpha)) + \Phi(g + (M_\alpha))$$

$$\Phi((f+(M_\alpha))\cdot(g+(M_\alpha))) = fg+f(M_\alpha)+g(M_\alpha)+(M_\alpha)^2 = fg = \Phi(f+(M_\alpha))\cdot\Phi(g+(M_\alpha))$$

notice

$$Im(\Phi) = K(\alpha)$$

but $k[x]/(M_\alpha)$ is a field so Φ is injective, so we have

$$k[x]/(M_\alpha) \cong \Phi(\underbrace{k[x]}_{\subseteq K} / \underbrace{(M_\alpha)}_{\ni\alpha}) \subseteq K[\alpha] \subseteq K(\alpha).$$

Therefore by definition of $K(\alpha)$,

$$\Phi(k[x]/(M_\alpha)) = K[\alpha] = K(\alpha).$$

$\square$

It's normal to abuse notation and write f for $f + I \in k[x]/I$

Example 2.4. *$\alpha = \sqrt{2}+\sqrt{3}$ can talk about $\mathbb{Q}(\sqrt{2}+\sqrt{3})$*

$$\alpha^2 = 5 + 6\sqrt{6} \qquad (\alpha^2-5)^2 = 24$$

so α is a root of $M = x^2 - 10x + 1 = 0$, need to check M is irreductable. Recall that a quartic can factor in two different ways

(i) (quadratic) $\times$ (quadratic)

(ii) (quadratic) $\times$ (linear)

(ii) $\Rightarrow$ root is a factor of 1

$$M(1) = -8 \qquad M(-1) = -8$$

M does not have a linear factor
(i)

$$\begin{aligned}(x^2+ax+b)(x^2+cx+d) &= x^4 - 10x^2 + 1\\ (x^2+ax+b)(x^2+cx+d) &= x^4(a+c)x^3(ac+b+d)x^2 + (bc+ad)x + bd\end{aligned}$$

$$\begin{array}{lcl} a+c=0 & \Rightarrow & a=-c\\ bd=1 & \Rightarrow & b=d,\ b=\pm1\\ ac+b+d=-10 & \Rightarrow & a^2 = 10+2b = 8 \text{ or } 12\end{array}$$

8 *or* 12 *not squares $\Rightarrow x^4 - 10x + 1$ is irreductable. So:*

$$\begin{aligned}\mathbb{Q}[x]/(x^4-10x+1) &\cong \mathbb{Q}(\sqrt{2}+\sqrt{3})\\ f &\mapsto f(\sqrt{2}+\sqrt{3})\end{aligned}$$

2.3 Degrees of extension

$L \supset K$ if we we say $l_1 + l_2$ and kl are defined but $l_1 l_2$ is not $\forall l_1, l_2 \in L$, $\forall k \in K$, this realises L as a vector space over K.

Definition 2.15. *The degree of L over K is just $dim(L)$ when L is thought of as a vector space over K. It is denoted*

$$[L : K]$$

Example 2.5. $\mathbb{C} \supset \mathbb{R}$

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} \quad \{1, i\} \text{ form a basis over } \mathbb{R}$$

So $[\mathbb{C} : \mathbb{R}] = 2$

Example 2.6. *Let* $f(x) = \sum_{i=0}^{d} a_i x^i$ *be an irreductable polynomial over* K

$$L = K[x]/(f) \supset K \qquad [L : K] = deg(f)$$

To show $B = \{1, x, \ldots, x^{d-1}\}$ *is a basis:*
Span:

$$x^d = \frac{-1}{a_d} \sum_{i=0}^{d-1} a_i x^i \Rightarrow x^d \in span(B)$$

similarly $x^n \in span(B)$ *for any* $n \geq d$

$$x^n = x^{n-d} x^d = x^{n-d} \left(\frac{-1}{a_d} \sum_{i=0}^{d-1} a_i x^i \right) \text{ is of degree } \leq n-1$$

and so $x^n \in span(B)$ *by induction, but* $\forall g \in K[x]/(f)$

$$g \in span(\{1, x, \ldots, x^n\}) \in span(\{1, x, \ldots, x^{d-1}\}) = span(B)$$

Linear Independence:
suppose $g(x) = \sum_{i=0}^{d} b_i x^i = 0$. *Then* $g \in (f)$ *but*

$$deg(g) \leq d - 1 \leq d = deg(f) \Rightarrow g = 0 \Rightarrow b_i = 0 \forall i$$

therefore if $f = M_\alpha$ *for some* α *algebraic over* K *then*

$$[k(\alpha) : K] = deg(M_\alpha)$$

Proposition 2.1. α *is algebraic over* K *iff* $[K(\alpha) : K] < \infty$

Proof.
$(\Rightarrow)$

$$[k(\alpha) : k] = deg(M_\alpha) < \infty$$

$(\Leftarrow)$
suppose

$$[k(\alpha) : k] = d < \infty$$

then $1, \alpha, \ldots, \alpha^d$ is linearly independant $\Rightarrow$ there exists a_i such that

$$\sum_{i=0}^{d} a_i \alpha^i = 0$$

□

Theorem 2.8 (Tower Theorem)**.** *suppose $K \subseteq L \subseteq M$ then*

$$[M : K] = [M : L][L : K]$$

Proof.
Let $\{a_i\}$ be a basis for L over K & let $\{b_i\}$ be a basis for M over L

Claim. *$\{a_i, b_i\}$ is a basis for M over K.*
Span: Let $v \in M$, then $\exists \lambda_i \in L$ such that

$$v = \sum_j \lambda_j b_j$$

$\exists m_{i,j} \in K$ such that $\lambda_j = \sum_i m_{i,j} a_i$ because $\lambda_i \in L$. So:

$$v = \sum_{i,j} m_{i,j} a_i b_j$$

Linear independance: suppose

$$\sum_{i,j} \underbrace{m_{i,j}}_{\in K} a_i b_j = 0$$

Let $\lambda_j = \sum_i m_{i,j} a_i$ then

$$\sum_i \lambda_j b_j = 0 \Rightarrow \lambda_j = 0 \quad \forall j$$

So

$$m_{i,j} = 0 \quad \forall i, j.$$

□

Corollary 2.2. *Let L be a field extention of K, $L \supseteq K$, and let $L^{alg} \subseteq L$ be the set of algebraic elements over K f L. Then L^{alg} is a field.*

Proof. Let $\alpha,\ \beta \in L^{alg}$ then

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$$

Let $\theta < \alpha + \beta, \alpha\beta, \alpha - \beta, \frac{\alpha}{\beta} \in K(\alpha, \beta)$, now:

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\theta)][K(\theta) : K]$$

therefore $[K(\theta) : K] < \infty$ so $\theta \in L^{alg}$ □

Example 2.7. *what is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$? Hopefully it's still $x^2 - 3$ note $\sqrt{2},\ \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*

$$(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$$

$$(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3}) = 11\sqrt{2} + 9\sqrt{3} - 9(\sqrt{2} + \sqrt{3}) = 2\sqrt{2} \quad \textit{so } \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = deg(x^4 - 10x^2 + 1) = 4$$

Therefore

$$4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}]$$

by theorem 2.8

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

Theorem 2.9 (Galois separability theorem)**.** *$K \subseteq \mathbb{C}$ and $f \in K[x]$ irreductable. Then f does not have repeated roots in $\mathbb{C}$.*

Proof. suppose α is a repeated root. Then

$$f(\alpha) = (x-\alpha)^2 g(x) \quad g \in \mathbb{C}[x]$$

$$f'(\alpha) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x)$$

So $f'(\alpha) = 0$ then $f' \in I(\alpha) = (f)$, but

$$deg(f') < deg(f) \Rightarrow f' = 0$$

Therefore f is constant, a contradiction. $\square$

Note. *This doesn't work over finite fields eg. $\mathbb{F}_p$:*

$$f = x^p - \alpha, \qquad f' = px^{p-1} = 0$$

Theorem 2.10 (Primitive element theorem)**.** *suppose $K \subseteq L \subseteq \mathbb{C}$ and $[L : K] < \infty$. Then $\exists \theta \in L$ such that*

$$L = K(\theta)$$

Proof. Let $\{1, \gamma_1, \ldots, \gamma_{d-1}\}$ be a basis for L over K. Then

$$L = K(\gamma_1, \ldots, \gamma_{d-1}) = K(\gamma_1, \ldots, \gamma_{d-2})K(\gamma_{d-1})$$

By induction on d we may assume that $k(\gamma_1, \ldots, \gamma_{d-2}) = K(\alpha)$. Let $\gamma_{d-1} = \beta$, now $L = K(\alpha, \beta)$. Let $p = M_\alpha,\ q = M_\beta$ and let

$$\begin{array}{ll} \alpha = \alpha_1, \ldots, \alpha_m & \text{be the roots of } p \text{ and} \\ \beta = \beta_1, \ldots, \beta_n & \text{be the roots of } q \end{array}$$

Choose c such that

$$\alpha_i + c\beta_j \neq \alpha + c\beta \quad \textit{unless } i = j = 1$$

To choose c we use:

(i) L is infinite

(ii) we have finitely many C's to avoid

(iii) Galois separability theorem 2.9 $\Rightarrow \alpha_i = \alpha_{i'} \Rightarrow i = i'$ and $\Rightarrow \beta_i = \beta_{i'} \Rightarrow i = i'$

Let $\theta = \alpha + c\beta$ we need to prove that

$$K(\theta) = k(\alpha, \beta)$$

Claim.

$$\beta \in K(\theta) \ \Rightarrow\ \alpha = \theta - c\beta \in K(\theta) \ \Rightarrow\ K(\alpha, \beta) \subseteq K(\theta) \subseteq K(\alpha, \beta)$$

Define $r(x) \in K(\theta)[x]$ by

$$r(x) = p(\theta - cx)$$

Then

$$r(\beta) = p(\theta - c\beta) = p(\alpha) = 0$$

on the other hand, $r(\beta_j) = p(\theta - c\beta_j) = 0$ *for* $j \geq 2$

$$\begin{aligned} &\Leftrightarrow \theta - c\beta_j = \alpha_i && \textit{for some } i \\ &\Leftrightarrow \alpha + c\beta = \alpha_i + c\beta_j && \textit{which never happens by choice of } c \end{aligned}$$

Now β *satisfies two polynomials over* $K(\theta)$*:*

$$q(\beta) = 0 \quad \& \quad r(\beta) = 0$$

We have just seen that β *is the only root that* q *and* L *have in common. Let* M *be the minimum polynomial of* β *over* $K(\theta)$

$$M|q \quad \textit{and} \quad M|r$$

So and root of M *is a root of* q *and* r *the only root of* M *is* β *so* $M = (x - \beta)^d$. $d = 1$ *by Galois separability theorem 2.9*

$$\Rightarrow M = x - \beta \Rightarrow \beta \in (\theta)$$

$\square$