Modern Algebra Lecture Notes: Rings and fields set 9, revision 3

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 27, 2010

Algebraic number

Let E be a field extension of F and let $a \in E$. We say a is algebraic over F if a is a root of some polynomial $f(x) \in F[x]$.

Minimum polynomial

If $a \in E$ is algebraic over F then the monic polynomial $f(x) \in F[x]$ of minimum degree having a as a root is called the minimum polynomial of a over F.

Example

If $F = \mathbb{Q}$, $E = \mathbb{Q}(2^{\frac{1}{5}})$ then $a = 2^{\frac{1}{5}}$ is algebraic over $\mathbb{Q}$ since $f(x) = x^5 - 2$ has $f(a) = 0$. This is irreducible over $\mathbb{Z}$ hence over $\mathbb{Q}$, so is the minimum polynomial of a.

Transcendental number

We say a is transcendental over F if a is **not** the root of any polynomial in $F[x]$.

Example

The number π is transcendental over $\mathbb{Q}$. The is a deep result. You will never see anything like $\pi^4 - 4\pi^3 - 45 = 0$. Then $\mathbb{Q}(\pi)$ behaves like the quotient field of the ring $\mathbb{Q}[x]$, i.e. like $\mathbb{Q}(x)$.

Definition

We say E is an algebraic extension of F if every element $a \in E$ is algebraic over F. If an extension is not algebraic it is called a transcendental extension. An extension of the form $F(a)$ is called a simple extension of F.

Theorem 36: Description of simple algebraic extensions

If $a \in E$ is algebraic over F then $F(a) \approx F[x]/\langle f(x) \rangle$ where $f(x)$ is the unique minimum polynomial of a over F which is necessarily irreducible over F.

Proof

If $f(a) = 0$ and $g(a) = 0$ with $f(x)$ and $g(x)$ being monic and having the same degree $n \geq 1$ then $h(x) = f(x) - g(x)$ satisfies $h(a) = 0$ and has degree less than n so must be the zero polynomial. Therefore the minimum polynomial $f(x)$ is unique.

If $f(x) = g(x).h(x)$ then $0 = f(a) = g(a)h(a)$ in E, but E is an integral domain. Therefore $g(a) = 0$ or $h(a) = 0$. But the degree of $f(x)$ is minimum with $f(a) = 0$. Therefore one of $g(x)$, $h(x)$ must be a unit, so $f(x)$ is irreducible over F.

Therefore $\langle f(x)\rangle$ is a maximal ideal and, as we have see above in Theorem 35, is the kernel of the mapping $\theta : F[x] \to F(a)$ defined by $g(x) \to g(a)$ with image $F(a)$ and giving an isomorphism $F(a) \approx F[x]/\langle f(x)\rangle$.

Definition

We have seen that E can be regarded as a vector space with scalars in F. We say the extension is finite if the dimension $[E : F] = n$ is finite.

Examples

(1) Since $x^2 - 3$ is irreducible over $\mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. The basis is $\{1, \sqrt{3}\}$.

(2) Since $x^n - 3$ is irreducible over $\mathbb{Q}$ we have $[\mathbb{Q}(3^{\frac{1}{n}} \cdot e^{\frac{2\pi i}{n}}) : \mathbb{Q}] = n$. The basis is $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a = 3^{\frac{1}{n}} \cdot e^{\frac{2\pi i}{n}}$.

Theorem 37: If $[E : F] = n < \infty$ then E is an algebraic extension of F

Proof

Let $a \in E$. The set of $n+1$ elements $\{1, a, a^2, \ldots, a^n\}$ must be linearly dependent, since otherwise the dimension of E over F would be necessarily greater than n.

Write down a linear dependence relation: $a_0 + a_1 a + \cdots + a_n a^n = 0$ with not all of the $a_i \in F$ zero. This shows the corresponding polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ has $f(a) = 0$ so a is algebraic over F. $\square$

The converse is false: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots) : \mathbb{Q}] = \infty$ but is algebraic.

Example

Since $[\mathbb{Q}(3^{\frac{1}{4}}) : \mathbb{Q}] = 4 < \infty$ every element of $\mathbb{Q}(3^{\frac{1}{4}})$ is algebraic over $\mathbb{Q}$.

Theorem 38: The set of algebraic numbers is a field

Statement

Let F be a field and E a field extension of F. Let $A \subset E$ be the set of elements of E which are algebraic over F. Then A is a field.

Proof

If $0 \neq a \in E$ has minimal polynomial $f(x)$ then $1/a$ has minimal polynomial $x^n f(1/x)$ where $n = \deg f(x)$.
If $a, b \in E$ are algebraic over F then b is algebraic over $F(a)$ so $[F(a,b) : F(a)] < \infty$ and $[F(a) : F] < \infty$ so, using the Dimension Theorem 39 below, $[F(a,b) : F] = [F(a,b) : F(a)][F(a) : F] < \infty$ so $F(a,b)$ is a finite hence algebraic extension of F making all of its elements algebraic, including $a.b$ and $a + b$.

Thus, if $a, b \in A$ so are $a + b$, $a.b$ and if $a \neq 0$ so is $1/a$. Hence A is a field. $\square$

If $F = \mathbb{Q}$ and $E = \mathbb{C}$ then any element in the field of algebraic numbers over $\mathbb{Q}$ is called an "algebraic number", just to make this subject confusing. It is often given the descriptive symbol $\mathbb{A}$.

Statement

Let $F \subset E \subset K$ be field extensions with $[E : F] = m < \infty$, $[K : E] = n < \infty$. Then $[K : F] < \infty$ also and $[K : F] = [K : E][E : F] = mn$.

Proof

Let $\{e_1, \ldots, e_m\}$ be a basis for E over F. Let $\{k_1, \ldots, k_n\}$ be a basis for K over E. Then in K we can form the subset of elements
$B := \{e_i \cdot k_j : 1 \leq i \leq m,\ 1 \leq j \leq n\}$.

B is a basis

Spanning: Let $x \in K$. Then, since $\{k_j\}$ is a basis for K over E, there exist $x_j \in E$ such that $x = \sum_j x_j k_j$.
Since $\{e_i\}$ is a basis for E over F, for each j there exist $f_{i,j} \in F$ such that $x_j = \sum_i f_{i,j} e_i$.

Then $x = \sum_j (\sum_i f_{i,j} e_i) k_j = \sum_{i,j} f_{i,j} e_i k_j$ so B spans K over F.

Completion of the proof of Theorem 39

Independence

Let $f_{i,j} \in F$ satisfy $\sum_{i,j} f_{i,j} e_i k_j = 0$. Then we can rearrange this to be

$$\sum_j (\sum_i f_{i,j} e_i) k_j = 0.$$

But the $\{k_j\}$ are linearly independent. Therefore for each j, $\sum_i f_{i,j} e_i = 0$. But the $\{e_i\}$ are also independent. Hence for all i, j, $f_{i,j} = 0$. This shows the $\{e_i k_j\}$ are linearly independent, and so B is a basis for K over F.

Since B is basis for K over F and the number of elements of B is mn, this is the dimension $[K : F] = mn = [K : E][E : F]$.$\square$

Statement

Let F have characteristic zero and let $a, b \in E$ be algebraic over F. Then there is an element $c \in E$ such that $F(a, b) = F(c)$. Consequently any finite algebraic extension is simple.

Example

Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $c = \sqrt{2} + \sqrt{3} \in E$. Since $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$ and $c^{-1} \in \mathbb{Q}(c)$ we have $\sqrt{3} - \sqrt{2} \in \mathbb{Q}(c)$, so therefore $\sqrt{3},\ \sqrt{2} \in \mathbb{Q}(c)$ and we get $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Minimal Polynomial

Again with $c = \sqrt{2} + \sqrt{3}$ we derive $(c - \sqrt{2})^2 = 3$ so $c^2 - 2\sqrt{2}c + 2 = 9 \implies (c^2 - 7)^2 = 8c^2$ giving $c^4 - 22c^2 + 49 = 0$, which is irreducible and thus the minimal polynomial for c over $\mathbb{Q}$. Hence

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

Let $f(x)$ be the minimum polynomial for a over F and suppose that $\{a = a_1, a_2, \ldots, a_m\}$ is a complete set of the distinct zeros for $f(x)$ in E. Let $g(x)$ be the minimum polynomial for b over F and suppose that $\{b = b_1, b_2, \ldots, b_n\}$ is a complete set of the distinct zeros for $g(x)$ in E. (We are assuming that E contains a splitting field for $f(x)$ and for $g(x)$.)

Since F has characteristic zero it contains a copy of $\mathbb{Q}$ and hence an infinite number of elements. Consider the finite set of ratios in E

$$\frac{a_i - a}{b - b_j},\ 1 \leq i \leq m,\ 2 \leq j \leq n$$

and choose a value $d \in F$ not equal to any of these elements.

Let $c = a + db$. This is a key definition, and shows how much flexibility there is in defining a primitive element. Then $c \in F(a, b)$ so $F(c) \subset F(a, b)$.

Define $h(x) = f(c - dx) \in F(c)[x]$. This is the other key definition. Then $h(b) = f(c - db) = f(a) = 0$ so $h(x)$ is divisible by the minimum polynomial, say $k(x)$, of b over $F(c)$.

Continuation of the Proof of Theorem 40, the Primitive Element

Since $g(b) = 0$, $g(x)$ is also divisible by $k(x)$ over $F(c)$. Hence any zero of $k(x)$ in E must also be a zero of both $h(x)$ and of $g(x)$.

But we know all of the zeros of $g(x)$. If $j > 1$

$$h(b_j) = f(c - db_j) = f(a + db - db_j) = f(a + d(b - b_j))$$

and this final argument to $f(x)$ is an a_i if and only if $a_i = a + d(b - b_j)$ or $d = (a_i - a)/(b - b_j)$ and d was chosen expressly to avoid this possibility. Therefore the only zero possible for $k(x)$ is $x = b$ and we can write in $F(c)[x]$, $k(x) = (x - b)^l$.

But $k(x)$, being a minimal polynomial, is irreducible so $l = 1$, and since $k(x) \in F(c)$, and $-b$ is a coefficient, $b \in F(c)$.

Hence $a = c - db \in F(c)$ so $F(a, b) \in F(c)$. Therefore $F(a, b) = F(c)$.$\square$

Example 1: $\mathbb{Q}(\sqrt{2})$

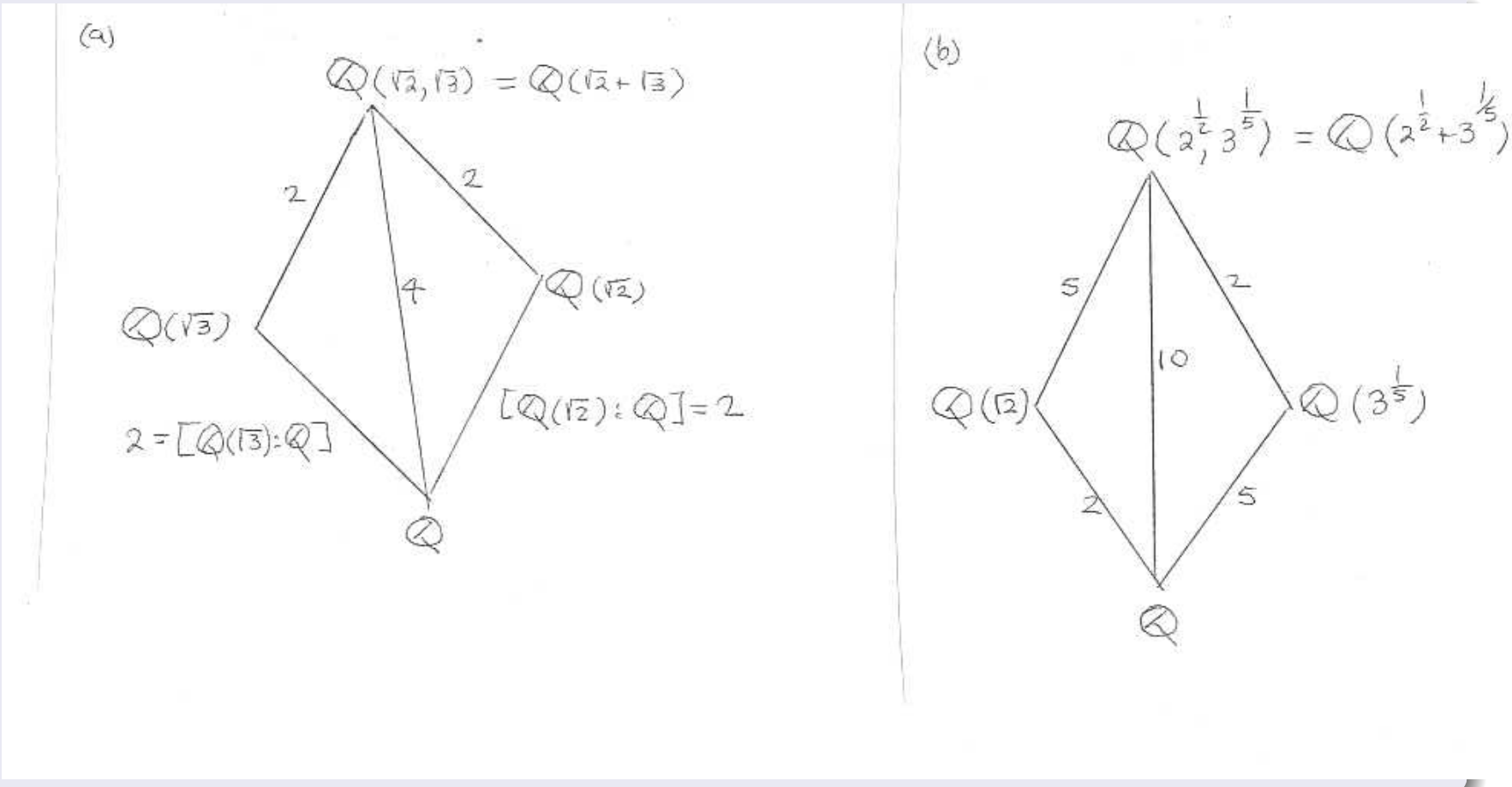
Let $a = \sqrt{2},\ f(x) = x^2 - 2,\ roots = \{a_1 = a = \sqrt{2}, a_2 = -\sqrt{2}\}$
and let $b = \sqrt{3},\ f(x) = x^2 - 3,\ roots = \{b_1 = b = \sqrt{3}, b_2 = -\sqrt{3}\}$

Then the values of the ratios for d in the Primitive Element Theorem are 0 when $a = a_1$ and

$$\frac{a_2 - a}{b - b_2} = \frac{-2\sqrt{2}}{2\sqrt{3}}$$

so we can choose d to be **any** non-zero rational number, set $c = \sqrt{2} + d\sqrt{3}$ and get $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(c)$.

Example (a): $\mathbb{Q}(\sqrt{2},\sqrt{3})$, (b) $\mathbb{Q}(2^{\frac{1}{2}},3^{\frac{1}{5}})$



Annotations to be justified

(a) We will show $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}] = 2$ and $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.

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

The minimum polynomial of $\sqrt{2}$ is $x^2 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Since this has degree 2 the result is immediate and the basis is $\{1, \sqrt{2}\}$, so all elements of $\mathbb{Q}(\sqrt{2})$ have the form $a + b\sqrt{2},\ \ a, b \in \mathbb{Q}$.

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

The minimal polynomial over $\mathbb{Q}$ for $\sqrt{3}$ is $x^2 - 3$. This is also irreducible over $\mathbb{Q}(\sqrt{2})$, a larger field. To see this, if it were not it would have a root in this field so we would have $\sqrt{3} = a + b\sqrt{2},\ \ a, b \in \mathbb{Q}$. Square this equation to get

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab},$$

which is impossible since $\sqrt{2}$ is irrational. Finally, since the degree of the minimal polynomial over $\mathbb{Q}(\sqrt{2})$ is 2 we have verified the dimension claim.

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

We can show this directly thus providing a check on the Dimension Theorem. If $\alpha=\sqrt{2}+\sqrt{3}$ (we have seen α is a primitive element for $\mathbb{Q}(\sqrt{2},\sqrt{3})$), then squaring and simplifying we get $\alpha^4-10\alpha^2+1=0$.

Irreducibility

The related polynomial $f(x)=x^4-10x^2+1$ is irreducible over $\mathbb{Z}$: any root β would need to divide 1 since $f(x)=(a_0+a_1x+a_2x^2+a_3x^3)(\beta-x)$ implies $a_0\beta=1$. Therefore $\beta=\pm1$, but $f(\pm1)\neq0$. Therefore $f(x)$ does not have a linear factor over $\mathbb{Z}$.

Quadratic factors ?

Any factor would need to be quadratic, say $f(x)=(x^2+\gamma x+1)(x^2+\delta x+1)$ or $f(x)=(x^2+\gamma x-1)(x^2+\delta x-1)$. Multiply out, say the first of these and equate the coefficients of x and x^2 gives $\gamma+\delta=0,\ \gamma\delta+2=-5$ so $\gamma^2=7$ which has no solution in $\mathbb{Z}$. Hence $f(x)$ is irreducible over $\mathbb{Z}$. Therefore it is irreducible over $\mathbb{Q}$ and we can say immediately, since $f(\alpha)=0$ that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$. A basis would be $\{1,\alpha,\alpha^2,\alpha^3\}$. An alternative basis is $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.