3. Polynomials and extensions

Let K be a field. Recall that $K[X]$ denotes the ring of polynomials in one formal variable X.

Let L be an extension of K, and consider any $u \in L$. We are interested in the extension $K(u)/K$. Our approach will be as follows. Consider $1, u, u^2, u^3, \ldots$. Either these are linearly independent over K or there exists n such that $u^n = a_{n-1}u^{n-1} + a_{n-2}u^{n-2} + \cdots + a_0 \cdot 1$ for some $a_0, \ldots, a_{n-1} \in K$. In the latter case, u is a root of $X^n - a_{n-1}X^{n-1} - \cdots - a_0 \in K[X]$.

Definition. If there exists a non-zero polynomial $f \in K[X]$ such that $f(u) = 0$, then we say that u is *algebraic* over K. Otherwise, u is said to be *transcendental* over K.

Definition. Suppose that u is algebraic over K. Then the *minimal polynomial* of u over K is the monic polynomial f of the smallest degree such that $f(u) = 0$. We write $f = \text{minpoly}_K(u)$.

(N.B. We will soon see that the minimal polynomial exists and is unique.)

Definition. The *evaluation map* $\epsilon_u \colon K[X] \to L$ is defined by $\epsilon_u(f) = f(u)$, $f \in K[X]$.

Lemma 3.1. *The evaluation map ϵ_u is a ring homomorphism.*

Proof. This is a routine check: for all $f, g \in K[X]$,

$$\epsilon_u(f+g) = (f+g)(u) = f(u) + g(u) = \epsilon_u(f) + \epsilon_u(g),$$
$$\epsilon_u(fg) = (fg)(u) = f(u)g(u) = \epsilon_u(f)\epsilon_u(g). \qquad \square$$

Therefore, $\ker \epsilon_u$ is an ideal of $K[X]$.

Proposition 3.2. *The element $u \in L$ is algebraic over K if and only if $\ker \epsilon_u \neq \{0\}$. In this case, the minimal polynomial f of u over K exists and is unique, and we have $\ker \epsilon_u = (f)$.*

Proof.

$$\begin{aligned}
&u \text{ is algebraic over } K && \Leftrightarrow\\
&f(u) = 0 \text{ for some non-zero } f \in K[X] && \Leftrightarrow\\
&f \in \ker \epsilon_u \text{ for some non-zero } f \in K[X] && \Leftrightarrow\\
&\ker \epsilon_u \neq \{0\}.
\end{aligned}$$

Now suppose $\ker \epsilon_u \neq \{0\}$. By Theorem 7 of the summary of prerequisites from "Polynomials and Rings", we have $\ker \epsilon_u = (f)$ for some monic polynomial $f \in K[X]$. Then, for any $h \in K[X]$, we have

$$h(u) = 0 \;\Leftrightarrow\; h \in \ker \epsilon_u = (f) \;\Leftrightarrow\; h \text{ is a multiple of } f. \tag{3.1}$$

This means that, $\deg f$ is the smallest amongst the degrees of non-zero polynomials of which u is a root; so f is a minimal polynomial of u over K. Further, suppose that h is another such minimal polynomial of u. Then $\deg h = \deg f$ and h is a multiple of f, whence $h = af$ for some $a \in K$. But also, h and f must both be monic, whence $a = 1$, and so $h = f$. □

Proposition 3.3. *Suppose that u is algebraic over K and f is its minimal polynomial. Then f is irreducible.*

Proof. Suppose $f = gh$ where g and h are non-constant. Then $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$. Then $0 = f(u) = g(u)h(u)$, so u is a root of either g or h. Without loss of generality, $g(u) = 0$. To summarise, $g(u) = 0$, $g \neq 0$ and $\deg(g) < \deg(f)$. But this contradicts the minimality of f, (We can make g monic by multiplying it by an appropriate scalar.) □

There is another useful description of what it means to be a minimal polynomial.

Proposition 3.4. *Let $u \in L$. Suppose u is a root of a monic and irreducible polynomial $f \in K[X]$. Then $f = \mathrm{minpoly}_K(u)$.*

Proof. Since $f \in \ker \epsilon_u$, we have $\ker \epsilon_u \neq \{0\}$, so u is algebraic. Let $g = \mathrm{minpoly}_K(u)$. Then g is not constant (as $g \neq 1$). But since $f \in \ker \epsilon_u = (g)$, we have $f = gh$ for some $h \in K[X]$. Since f is irreducible and g is non-constant, this implies $f = ag$ for some $a \in K$. But f and g are both monic, so $f = g$. □

Proposition 3.5. *Let $f \in K[X]$. Suppose that $2 \leq \deg(f) \leq 3$. Then f is irreducible over K if and only if f has no root in K.*

Proof. If f has a root $a \in K$, then $X - a$ divides f, so f is reducible. Conversely, if f is reducible, then $f = gh$ for some non-constant $g, h \in K[X]$. Since $3 \geq \deg(f) = \deg(g) + \deg(h)$, at least one of g and h has degree 1, say g. Then $g = b \cdot (X - a)$ for some $a, b \in K$ with $b \neq 0$, so a is a root of g and hence of f. □

Now we are able to find minimal polynomials in some cases.

Examples.

$u \in \mathbb{C}$	algebraic over $\mathbb{Q}$?	$\text{minpoly}_{\mathbb{Q}}(u)$ (if algebraic)
$1/2$	yes	$X - 1/2$
$\sqrt{3}$	yes	$X^2 - 3$
i	yes	$X^2 + 1$
$\sqrt[3]{2}$	yes	$X^3 - 2$
e	no (hard: Hermite's thm)	
π	no	
$e + \pi$	not known	
$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$	yes	$X^2 + X + 1$

Lemma 3.6. *Let $u \in L$ be algebraic over K. Then $\operatorname{im} \epsilon_u = K(u)$.*

Proof. Let $f = \text{minpoly}_K(u)$. Let $F = \operatorname{im} \epsilon_u$. By the First Isomosphism Theorem, the map $\bar{\epsilon}_u \colon K[X]/(f) \to F$, defined by $\bar{\epsilon}_u(g + (f)) = \epsilon_u(g)$ for $g + (f) \in K[X]/(f)$, is a ring isomorphism between $K[X]/(f)$ and F. Since f is irreducible over K, $K[X]/(f)$ is a field, whence F is also a field. Moreover, F contains u because $u = \epsilon_u(X)$, and $F \supseteq K$ because $\epsilon_u(a) = a$ for all $a \in K$. Hence, $F \supseteq K(u)$.

Conversely, for any polynomial $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$, we have $\epsilon_u(f) = a_n u^n + \cdots + a_1 u + a_0 \in K(u)$ because $K(u)$ is closed under addition and multiplication. So $F \subseteq K(u)$, whence $F = K(u)$. □

Theorem 3.7. *Let $K \subseteq L$ be fields and $u \in L$. The following are equivalent:*

(i) The element u is algebraic over K, with minimal polynomial of degree n;

(ii) The extension $K(u)/K$ is finite, with $[K(u) : K] = n$.

Moreover, if (i) (or (ii)) holds, then $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis of $K(u)$ over K.

Proof. (i) $\Rightarrow$ (ii). Let $f = \text{minpoly}_K(u)$ (so that $\deg(f) = n$). We claim that $T = \{1, u, u^2, \ldots, u^{n-1}\}$ is a basis of $K(u)$.

First, we show that $K(u) = \operatorname{im} \epsilon_u$ is spanned by T over K. Indeed, let $g \in K[X]$. By the Euclidean property, $g = qf + r$ for some $q, r \in K[X]$ with $\deg(r) < n$. Thus,

$$\epsilon_u(g) = g(u) = q(u)f(u) + r(u) = r(u).$$

But $r = a_m X^m + \cdots + a_0$ for some $m < n$ and $a_0, \ldots, a_m \in K$, so $r(u) = a_m u^m + \cdots + a_0$ belongs to the span of T over K. Thus, T spans $\operatorname{im} \epsilon_u = K(u)$ over K.

Secondly, we prove that T is linearly independent over K. Indeed, suppose (for contradiction) that $a_{n-1} u^{n-1} + a_{n-2} u^{n-2} + \cdots + a_0 = 0$ for some

$a_{n-1}, \dots, a_0 \in K$ which are not all zero. Then $h = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in K[X]$ is not zero and $h(u) = 0$. Since $\deg(h) < n$, this is a contradiction to the fact that $f = \operatorname{minpoly}_K(u)$.

Note that we have proved the last statement of the theorem as well.

(ii) $\Rightarrow$ (i). Since $n = [K(u) : K]$, the elements $1, u, u^2, \dots, u^n$ must be linearly dependent over K. That is, $a_n u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$ for some $a_0, \dots, a_n \in K$, not all zero. So u is a root of the non-zero polynomial $w = a_n X^n + \cdots + a_0 \in K[X]$. Thus u is algebraic. We have already proved that in this case $[K(u) : K] = \deg(\operatorname{minpoly}_K(u))$. □

Remark. This proof suggests a way of finding the minimal polynomial of u in some situations. We consider $1, u, u^2, \dots$ and find the *smallest* n such that $1, u, \dots, u^n$ are linearly dependent (assuming such an n exists). More specifically, we find the coefficients $a_0, \dots, a_{n-1}$ such that $u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$. Then $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ is the minimal polynomial of u over K. [N.B. This is not the only way to find minimal polynomials: we have already seen other ways, and we will see more. Use your judgement to select the best approach for each particular problem!]

Corollary 3.8. *Let L/K be a field extension. Suppose $L = K(u_1, \dots, u_k)$ for some $u_1, \dots, u_k \in L$. For each $i = 1, \dots, k$, assume that the extension $K(u_i)/K$ is finite, and write $n_i = [K(u_i) : K]$. Then L/K is finite and $[L : K] \le n_1 n_2 \cdots n_k$.*

Proof. We argue by induction on k. If $k = 1$, the result holds by Theorem 3.7. Let $M = K(u_1, \dots, u_{k-1})$. Then $[M : K] \le n_1 \cdots n_{k-1}$ by the inductive hypothesis. Since $K(u_k)/K$ is finite, the element u_k is algebraic over K. Moreover, $g = \operatorname{minpoly}_K(u_k)$ has degree $n_k = [K(u_k) : K]$ (by Theorem 3.7). Now $g \in M[X]$ and $g(u_k) = 0$, so u_k is algebraic over M and $\deg(\operatorname{minpoly}_M(u_k)) \le n_k$. Hence, $[L : M] \le n_k$ (by Theorem 2.14). Thus, by Tower Law, $[L : K]$ is finite and

$$[L : K] = [L : M][M : K] \le n_k(n_1 \cdots n_{k-1}) = n_1 \cdots n_k. \qquad \square$$

Corollary 3.9. *Let L/K be a finite field extension. Then every element of L is algebraic over K.*

Corollary 3.10. *Let L/K be any field extension. Let F be the set of the elements of L that are algebraic over K. Then F is a subfield of L.*

Proof. Clearly, $0, 1 \in F$. Let $u, v \in F$, and consider the subfield $K(u, v)$ of L. Since u, v are algebraic over K, the extensions $K(u)/K$ and $K(v)/K$ are finite by Theorem 3.7. But then $K(u, v)/K$ is finite by Corollary 3.8. By Theorem 3.7 again, this implies that every element of $K(u, v)$ is algebraic over K, so $K(u, v) \subseteq F$. In particular, $u + v, uv \in F$; and if $v \neq 0$, then $v^{-1} \in F$. Hence, F is a subfield of L. □

For example, the set $\bar{\mathbb{Q}}$ of all complex numbers that are algebraic over $\mathbb{Q}$ is a field: $\bar{\mathbb{Q}}$ is called the field of *algebraic numbers*.