2.A Field Extensions

Recall that a field k is a commutative ring $(k, +, \cdot)$ (with multiplicative identity $1 = 1_k$) such that the non zero elements $k^* = k \setminus \{0\}$ form a group under multiplication.

If k, K are fields with $k \subseteq K$, i.e. k is a subfield of K, then K is called a field extension of k and is denoted by K/k; the field k is called the base field. Let K/k be a field extension. Then the field K is a k-vector space with scalar multiplication $k \times K \longrightarrow K$ $(a, x) \longmapsto ax$ = the multiplication of a and x in K. We write $[K : k]$ for the dimension $\dim_k K$ of the k-vector space K and is called the degree of the field extension K/k. If $[K : k]$ is finite, then K/k is called a finite extension; otherwise K/k is an infinite extension.

2.A.1 Example The fields of rational numbers, real numbers and complex numbers will be denoted by $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, respectively. For a prime number p, the field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p will be denoted by $\mathbb{F}_p$. The fields $\mathbb{Q}$ and $\mathbb{F}_p$ are called prime field and often appear as the base fields.

The characteristic (Charak) of a field k is either 0 or a prime number $p > 0$; (Either) $\mathbb{Q} \subseteq k$ or $\mathbb{F}_p \subseteq k$ depending on whether the characteristic of k is 0 or $p > 0$.

Therefore, if K/k is a field extension, then $\operatorname{char} K = \operatorname{char} k$

Finite field extensions of $\mathbb{Q}$ are called <u>algebraic number fields</u> and are one of the objects of study in algebraic number theory.

2.A.2 Example (<u>Rational function fields</u>) Let k be a field and let $k[X]$ be the polynomial ring over k in one indeterminate X. The quotient field of $k[X]$ consists of

$$\{ f/g \mid f, g \in k[X],\ g \neq 0 \}$$

and is called the <u>rational function field</u> in X over k denoted by $k(X)$.

More generally, the quotient field of the polynomial ring $k[X_1, \cdots, X_n]$ over k in n (independent) indeterminates $X_1, \cdots, X_n$ is called the <u>rational function field</u> in $X_1, \cdots, X_n$ over k and is denoted by $k(X_1, \cdots, X_n)$. Field extensions of a rational function field arise often in <u>algebraic geometry</u> and in the <u>theory of division rings</u>.

2.A.3 Example (<u>Field of Laurent series</u>) Let k be a field and let $k[\![X]\!]$ be the formal power series ring over k in one indeterminate X. The quotient field of $k[\![X]\!]$ consists of $\left\{ \sum_{n \geq n_0} a_n X^n \mid n_0 \in \mathbb{Z},\ a_n \in k \right\}$ and is called the <u>field of Laurent series</u> in X over k and is denoted by $k((X))$. Similarly, $k((X_1, \cdots, X_n))$.

2.A.4 Example (*Generators of fields*) In order to study the roots of a polynomial over a field k, we shall consider a minimal field extension of k tha contain all the roots of the polynomial. In intuitive terms, this field extension is generated by k and th roots. More precisely:

Let K/k be a field extension and let $\underline{x} \subseteq K$. The *ring generated by* $\underline{x}$ and k (or the *k-subalgebra of K generated* by $\underline{x}$) is the smallest subring of K that contain $\underline{x}$ and k (or the smallest k-subalgebra of K that contain $\underline{x}$); it is the intersection of all subrings of K that contain $\underline{x}$ and k (or the intersection of all k-subalgebras of K that contain $\underline{x}$) and is denoted by $k[\underline{x}]$. The *field generated by* $\underline{x}$ *and* k is the quotient field of $k[\underline{x}]$ and is denoted by $k(\underline{x})$; this is the intersection of all subfields of K that contain $\underline{x}$ and k.

For example, if $\underline{x} = \{x\}$, then $k[x] = k[\{x\}] = \{f(x) \mid f \in k[X]\}$ is the image of the *evaluation* or *substitution* homomorphism $\varphi_x : k[X] \longrightarrow K$, defined by $X \longmapsto x$. Further,

$$k(x) = k(\{x\}) = \left\{ f(x)/g(x) \;\middle|\; f, g \in k[X],\ g(x) \neq 0 \right\}.$$

Similarly, if $\underline{x} = \{x_1, \cdots, x_n\}$, then $k[x_1, \cdots, x_n] = k[\{x_1, \cdots, x_n\}] = \{f(x_1, \cdots, x_n) \mid f \in k[X_1, \cdots, X_n]\}$ is the image of the evaluation map $\varphi_{x_1, \cdots, x_n} : k[X_1, \cdots, X_n] \longrightarrow K$, $X_i \longmapsto x_i$, $i = 1, \cdots, n$ and

$$k(x_1, \cdots, x_n) = k(\{x_1, \cdots, x_n\}) = \left\{ \frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)} \;\middle|\; \begin{array}{l} f, g \in k[X_1, \cdots, X_n], \\ g(x_1, \cdots, x_n) \neq 0 \end{array} \right\}.$$

Moregenerally, if $\underline{x}$ is an arbitrary subset of K and if $y \in k[\underline{x}]$ (resp. $y \in k(\underline{x})$), then there exis a finite subset $\{x_1, \cdots, x_n\}$ of $\underline{x}$ such that $y \in k[x_1, \cdots, x_n]$ (resp. $k(x_1, \cdots, x_n)$). Therefore

$$k[\underline{x}] = \bigcup \{k[x_1, \cdots, x_n] \mid \{x_1, \cdots, x_n\} \subseteq \underline{x}\} \text{ and}$$

$$k(\underline{x}) = \bigcup \{k(x_1, \cdots, x_n) \mid \{x_1, \cdots, x_n\} \subseteq \underline{x}\},$$ where the union runs through all finite subsets of $\underline{x}$.

Special Cases: The extension $\mathbb{C}/\mathbb{R}$ is a finite extensio since $\{1, i\}$ is a $\mathbb{R}$-basis of $\mathbb{C}$. Therefore $[\mathbb{C} : \mathbb{R}] = 2$ an $\mathbb{C} = \mathbb{R}(i)$ is generated by $\{i\}$ over $\mathbb{R}$. Both the field extensi $\mathbb{C}/\mathbb{Q}$ and $\mathbb{R}/\mathbb{Q}$ are infinite. For $x \in \mathbb{C}$, the field extension $\mathbb{Q}(a)/\mathbb{Q}$ can be finite or infinite depending on x. For instance, if $x = \sqrt{-1} = i$ or $x = e^{2\pi i/n}$, $n \in \mathbb{N}^*$, then $\mathbb{Q}(x)/\mathbb{Q}$ is finite (see). Further, note that the field extensions $\mathbb{Q}(\pi)/\mathbb{Q}$ and $\mathbb{Q}(e)/\mathbb{Q}$ are not finite.

2.A.5 Example Let k be a field and let $K = k($; be the field of rational functions in X over k. Let $f \in K$, $f \neq 0$ and let $L = k(f)$ be the set of all rational functions in f over k, i.e. $L = k(f) = \left\{ F(f)/G(f) \right.$ $\left. F, G \in K, G(f) \neq 0 \right\}$.

(1) If $f = t^2$, then K/L is an extension of degree 2; in fact $\{1, t\}$ is a L-basis of K.

(2) More generally, if f is non-constant, i.e. $f \notin k$, then the field extension K/L is finite of degree

$\max\{\deg F, \deg G\}$, where $f = F/G$ with F, $G \neq 0$ and $\gcd(F, G) = 1$.

Remark **Lüroth's theorem** states that: every field L with $k \subseteq L \subseteq K$ is of the form $L = k(f)$ for some $f \in K$.

2.A.6 Example Let $p(X) \in k[X]$ be an irreduci. polynomial of degree d. Then $L = k[X]/(p(X))$ is a field extension of k of degree d. Note that $L = k[x]$, where x is the image of X in L under the canonical surjective K-algebra homomorphism $k[X] \longrightarrow L$, i.e. L is a finitely generated k-algebra over k. Moreover, it follows from the division algorithm for polynomials that $\{1, x, \dots, x^{d-1}\}$ is a basis of L over k. Therefore $[L : k] = d = \deg p(x$

Special cases:

(1) Let $a \neq \pm 1$ be a square free integer. Then the polynomial $p(X) = X^n - a \in \mathbb{Q}[X]$ is irreducible (use Eisenstein's criterion for every $n \in \mathbb{N}, n \geq 2$) and hence $L = \mathbb{Q}[X]/(X^n - a$ is a field extension of $\mathbb{Q}$ of degree n.

(2) Let p be a prime number. Then the p-th cyclotomic polynomial

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

is irreducible over $\mathbb{Q}$ and hence $\mathbb{Q}(\zeta_p) := \mathbb{Q}[X]/(\Phi_p(X$ is a finite field extension of $\mathbb{Q}$ of degree $p-1$. This field extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is called the p-th cyclotomic extension

2.A.7 Example Let k be a field and let K be a finitely generated field extension of k, i.e. $K = k(x_1, \cdots, x_n)$ for some $x_1, \cdots, x_n \in K$. We can break up the extension K/k into a collection of subextension that are easier to analyse (see

Let $L_i = k(x_1, \cdots, x_i) \subseteq K$, $i = 1, \cdots, n$ and $L_0 := k$

Then we have a chain of fields

$$k = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = K$$

with $L_{i+1} = L_i(x_{i+1})$ is a simple extension of L_i, $i = 0, \cdots, n-1$.

To make this idea of decomposing K/k into these subextensions useful, we need to have transitivity results that tell us how to translate information about subextensions to the full extension K/k. We will prove a number of transitivity results in these notes. The first one dealing the most basic invariant of a field extension, namely, the degree of a field extension, is the following:

Degree formula: Let $K \subseteq L \subseteq K$ be fields. Then

$$[K : k] = [K : L][L : k].$$

Proof Let $\{x_i \mid i \in I\}$ be a basis of L over k and let $\{y_j \mid j \in J\}$ be a basis of K/L. Then we will show that the set $\{x_i y_j \mid (i, j) \in I \times J\}$ is a basis of K over k.

Let $x \in K$, then $x = \sum_{j \in J} \alpha_j y_j$ for some $\alpha_j \in L$ with $(\alpha_j)_{j \in J} \in L^{(J)}$, i.e. only finitely many $\alpha_j \neq 0$. But each non-zero α_j can be written as $\alpha_j = \sum_{i \in I} \beta_{ij} x_i$ for some $\beta_{ij} \in k$ with only finitely many $\beta_{ij} \neq 0$ for each j.

Therefore $x = \sum_{j \in J} \alpha_j y_j = \sum_{j \in J} \left(\sum_{i \in I} \beta_{ij} x_i \right) y_j = \sum_{(i,j) \in I \times J} \beta_{ij} x_i y$

This proves that the k-vector space K is generated by $\{x_i y_j \mid (i,j) \in I \times J\}$. For linear independence, if $\sum_{(i,j)\in I\times J} \beta_{ij} x_i y_j = 0$ with $\beta_{ij} \in k$ and only finitely many $\beta_{ij} \neq 0$, then $\sum_{j\in J}\left(\sum_{i\in I} \beta_{ij} x_i\right) y_j = 0$ (by the independence of $y_j, j\in J$ over L, we have) $\sum_{i\in I} \beta_{ij} x_i = 0$ for each $j \in J$. Now, the independence of $x_i, i\in I$ over k, shows that $\beta_{ij} = 0$ for all $(i,j) \in I\times J$. This proves that $\{x_i y_j \mid (i,j) \in I\times J\}$ is a basis of K over l. Therefore $[K:k] = |I\times J| = |I|\cdot|J| = [K:L][L:k]$

The main interest in this section is the study of algebraic field extensions K/k, i.e. in which every element $x \in K$ satisfies a non-zero polynomial equation with coefficients in k.

2.A.8 Definition Let K/k be a field extension. An element $x \in K$ is said to be algebraic over k if there exists a non-zero polynomial $f \in k[X]$ such that $f(x)=0$. An element $x \in K$ is said to be transcendental over k if x is not algebraic over k.

An element $x \in K$ is algebraic over k if and only if the kernel $\mathfrak{o}_x$ of the subsitution homomorphism $k[X] \xrightarrow{\varphi_x} K$, $X \longmapsto x$ is non-zero. The (uniquely determined) monic polynomial which generates the ideal $\mathfrak{o}_x$ is called the minimal polynomial of x over k and is denoted by $\mu_{x,k}$ or just μ_x.

2.A.9 Example. The imaginary unit i is algebraic over $\mathbb{Q}$, since $i^2+1=0$. Further, since $i \notin \mathbb{Q}$, $\mu_i = X^2+1$ is the minimal polynomial of i over $\mathbb{Q}$. Note that X^2+1 is also the minimal polynomial of i over $\mathbb{R}$, but $X-i$ is the minimal polynomial of i over $\mathbb{C}$. Therefore the minimal polynomial of an element depends on the base field; also whether the element is algebraic or transcendental depends on the base field.
If $\zeta_n = e^{2\pi i/n} = \cos 2\pi/n + i \sin 2\pi/n$, then $\zeta_n^n - 1 = 0$ and hence ζ_n is algebraic over $\mathbb{Q}$. The determination of $\mu_{\zeta_n,\mathbb{Q}}$ is non-trivial and will be done in

2.A.10 Example In 1873, Hermite proved that the Euler-number e is transcendental over $\mathbb{Q}$ and 9 years later, Lindemann proved that π is transcendental over $\mathbb{Q}$. It is unknown if e is transcendent over $\mathbb{Q}(\pi)$.

The minimal polynomial of an element and the degree of a field extension are two of the most basic tools used in the study of algebraic extensions. The following proposition gives a relation between them.

2.A.11 Proposition Let K/k be a field extension and let $x \in K$ be algebraic over k. Then:

(1) The polynomial $\mu_x \in k[X]$ is irreducible over k.

(2) For $g(X) \in k[X]$, $g(x)=0$ if and only if μ_x divide g in $k[X]$.

(3) If $n = \deg \mu_x$, the the elements $1, x, \cdots, x^{n-1}$ form a basis for $k(x)$ over k. In partiular, $k(x)$ is finite over k and $[k(x):k] = \deg \mu_x$.

Proof Since x is algebraic over k, $\mu_x \neq 0$, in fact $\deg \mu_x \geq$ and $\mathfrak{p}_x = (\mu_x)$ is the kernel of the substitution homomorphism $\varphi_x : k[X] \longrightarrow K$, $X \longmapsto x$. In particular, induces an isomorphism $k[X]/(\mu_x) \xrightarrow{\simeq} k[x] \subseteq K$ of k-algebras.

(1) Since $k[x]$ is a subring of a field K, $k[x]$ is an integral domain and hence μ_x is a prime element in $k[X]$ in particular, μ_x is irreducible over k.

(2) Let $g \in k[X]$. Then by division algorithm we have

$g = q \cdot \mu_x + r$ with $q, r \in k[X]$ and $\deg r < \deg \mu_x$

Therefore, since $\mu_x(x) = 0$, we have $g(x) = q(x)\mu_x(x) + r(x)$
$= r(x)$. Therefore $g(x) = 0$ if and only if $r(x) = 0$ or
equivalently, $r = 0$, (since $\deg r < \deg \mu_x$), i.e. $g = q \cdot \mu_x$

(3) Since $\mathfrak{p}_x = (\mu_x) \neq 0$ prime ideal in a PID $k[X]$,
$\mathfrak{p}_x$ is a maximal ideal in $k[X]$, i.e. $k[x] \cong k[X]/\mathfrak{p}_x$
is a field, in particular, $k[x] = k(x)$. Now, by 2.A.6
$1, x, \dots, x^{n-1}$ is a k-basis of the vector space $k[x] = k(x$

2.A.12 Corollary Let K/k be a field extension and
let $x \in K$. Then the following statements are equivale
(i) x is algebraic over k.
(ii) $k[x]$ is a finite dimensional vector space over k of
dimension $\deg \mu_x = n$.
(iii) $k[x]$ is a field.
(iv) $k(x) = k[x]$.

Proof (i) $\Rightarrow$ (ii) : proved in (3) of 2.A.11.
(ii) $\Rightarrow$ (iii) : Let $y \in k[x]$, $y \neq 0$. Then (λ_y : the left multiplicati
$x^i \longmapsto yx^i$, $i = 0, \dots, n-1$, is an injective (endomorphism of k-vecto
space $k[x]$ and since $\dim_k k[x] = n < \infty$, λ_y is surjecti
in particular, $1 = y \cdot z$ for some $z \in k[x]$. This proves
that $z = y^{-1}$ in $k[x]$.
(iii) $\Rightarrow$ (iv): $k(x)$ = the quotient field of $k[x]$.
(iv) $\Rightarrow$ (i) : $\frac{1}{x} \in k(x) = k[x]$. Therefore $\frac{1}{x} = g(x)$ for
some $g \in k[X]$ and hence $1 = xg(x) = (Xg)(x)$, i.e.
$(1 - Xg)(x) = 0$, i.e. x satisfies a non-zero polynomial
$1 - Xg \in k[X]$, i.e. x is algebraic over k.

2.A.13 Corollary Let K/k be a field extension and let $x_1, \dots, x_n \in K$ be algebraic over k. Then $k[x_1, \dots, x_n]$ is a finite field extension of k of degree

$$[k[x_1, \dots, x_n] : k] \leq \prod_{i=1}^{n} [k(x_i) : k] = \prod_{i=1}^{n'} \deg$$

Proof We prove this by induction on n; the case $n=1$ follows from 2.A.12. Now assume $n \geq 2$ and put $L := k[x_1, \dots, x_{n-1}]$, then by induction hypothesis L is a field and $[L : k] \leq \prod_{i=1}^{n-1} [k(x_i) : k]$. Further, since x_n is algebraic over k, it is algebraic over L and $\mu_{x_n, L}$ divides $\mu_{x_n, k}$. Therefore $k[x_1, \dots, x_n] = L[x_n$ is a field and $[k[x_1, \dots, x_n] : L] \leq [k(x_n) : k] = \deg \mu_{x_n,}$ Therefore by degree formula and the induction hypothesi

$$[k[x_1, \dots, x_n] : k] = [k[x_1, \dots, x_n] : L][L : k] \leq \prod_{i=1}^{n} [k[x_i) : k$$

$$\leq \prod_{i=1}^{n} \deg \mu_{x_i, k}$$

2.A.14 Definition A field extension K/k is called a *algebraic extension* if every element of K is algebra over k.

For example k/k is algebraic extension. $\mathbb{C}/\mathbb{R}$ is an algebraic extension, since every $z \in \mathbb{C}$ satisfies a real polynomial $X^2 - (z + \bar{z})X + z\bar{z} \in \mathbb{R}[X]$.

2.A.15 Proposition Let K/k be a field extension and let $x_1, \dots, x_n \in K$. Then the following statements are equivalent:

(i) $x_1, \dots, x_n$ are algebraic over k

(ii) $k(x_1, \dots, x_n)/k$ is a finite extension of deg $\leq \prod_{i=1}^{n} \deg \mu_{x_i}$

(iii) $k(x_1,\cdots,x_n)\,|\,k$ is an algebraic extension.

Proof (i) $\Rightarrow$ (ii): proved in 2.A.13.

(ii) $\Rightarrow$ (iii): Let $y \in k(x_1,\cdots,x_n)$. Then $k \subseteq k(y) \subseteq k(x_1,\cdots,$ and hence $[k(x_1,\cdots,x_n):k(y)]\,[k(y):k] = [k(x_1,\cdots,x_n):k] <$ Therefore $[k(y):k] < \infty$ and hence y is algebraic over k by 2.A.12.

(iii) $\Rightarrow$ (i): Trivial.

2.A.16 Corollary Every finite field extension is an algebraic extension.

2.A.17 Corollary Let K/k be a field extension and let $\underline{x} \subseteq K$ be a subset of K such that each element of $\underline{x}$ is algebraic over k. Then the field extension $k(\underline{x})/k$ is an algebraic extension. Moreover, if $\underline{x}$ is a finite subset, then $k(\underline{x})/k$ is a finite extension.

Proof Let $y \in k(\underline{x})$. Then $y \in k(x_1,\cdots,x_n)$ for some $x_1,\cdots,x_n \in \underline{x}$ and hence y is algebraic over k by 2.A.15. The last part is also clear from 2.A.15.

We are now ready to prove that the property of being algebraic is transitive. This result will be used very often. In the case of finite extensions, the transitivity follows from the degree formula in 2.A.7 and 2.A.16, but it is harder to prove for general extensions.

2.A.18 Corollary Let $k \subseteq L \subseteq K$ be field extensions. If L/k and K/L are algebraic, then K/k is also algebraic.

Proof Let $x \in K$ and let $\mu_{x,L} = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in L[X]$ be the minimal polynomial of x over L. Since L/k is algebraic and $a_0, \cdots, a_{n-1} \in L$, by 2.A.15 $L_0 := k(a_0, \cdots, a_{n-1})$ is a finite (and hence algebraic) extension of k. Further, since $\mu_{x,L} \in L_0[X]$ and $\mu_{x,L}(x) = 0$, x is algebraic over L_0. Therefore $L_0(x) \mid L_0$ is finite and also by degree formula $[L_0(x) : k] = [L_0(x) : L_0][L_0 : k]$, i.e. $L_0(x)/k$ is a finite extension. Now, since $k(x) \subseteq L_0(x)$, $k(x)/k$ is a finite extension and hence x is algebraic over k by 2.A.12.

Now we can describe the set of algebraic elements in a field extension.

2.A.19 Definition Let K/k be a field extension. The set $\{x \in K \mid x \text{ is algebraic over } k\}$ is called the *algebraic closure* of k in K.

2.A.20 Corollary Let K/k be a field extension and let K' be the algebraic closure of k in K. Then K' is a field and hence is the largest algebraic extension of k contained in K.

Proof Let $x, y \in K'$. Then it is enough to prove that $x \pm y$, $x \cdot y$ and x/y belong to K', i.e. they are algebraic over k. Since x and y are algebraic over k, the field extension $k(x,y)/k$ is algebraic by 2.A.15 and hence