Field Extensions

Def. A field E is an **extension field** of a field F if F is a subfield of E $(F \leq E)$.

Ex. $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\mathbb{C}$ is an extension field of $\mathbb{R}$ and $\mathbb{Q}$.

Kronecker's Theorem: Let F be a field and let $g(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $g(\alpha) = 0$.

Ex. Let $F = \mathbb{R}$ and let $g(x) = x^2 + 1$. $g(x)$ has no zeros in $\mathbb{R}$ and thus is irreducible over $\mathbb{R}$. $< x^2 + 1 >$ is a maximal ideal in $\mathbb{R}[x]$ so $\mathbb{R}[x]/< x^2 + 1 >$ is a field.

We can view $\mathbb{R}$ as a subfield of $\mathbb{R}[x]/< x^2 + 1 >$ through the mapping:

$$\varphi: \mathbb{R} \to \mathbb{R}[x]/< x^2 + 1 > \text{ by } \varphi(t) = t + < x^2 + 1 >, \ t \in \mathbb{R}.$$

Let $\alpha = x + < x^2 + 1 > \in \mathbb{R}[x]/< x^2 + 1 >$,

then $\alpha^2 + 1 = (x + < x^2 + 1 >)^2 + (1 + < x^2 + 1 >)$

$$= (x^2 + 1) + < x^2 + 1 >$$

$$= 0.$$

Thus α is a zero of $x^2 + 1$. So we can think of $\mathbb{R}[x]/< x^2 + 1 >$ as an extension field of $\mathbb{R}$, which has an element α where $\alpha^2 + 1 = 0$.

Ex. Let $F = \mathbb{Q}$ and consider $f(x) = x^4 - 7x^2 + 10$.

In $\mathbb{Q}[x]$, $f(x) = (x^2 - 2)(x^2 - 5)$, where $x^2 - 2$ and $x^2 - 5$ are irreducible over $\mathbb{Q}$.

We can construct a field $\mathbb{Q}[x]/ < x^2 - 2 >$, which can be thought of as an extension field of $\mathbb{Q}$, which has an element α such that $\alpha^2 - 2 = 0$ (just let $\alpha = x + < x^2 - 2 >$).

We can also construct an extension field of $\mathbb{Q}$, $\mathbb{Q}[x]/ < x^2 - 5 >$, which has an element α such that $\alpha^2 - 5 = 0$.

Def. An element α of an extension field E of a field F is **algebraic** over F if $f(\alpha) = 0$ for some $f(x) = F[x]$. If α is not algebraic over F, then α is **transcendental** over F.

Ex. $\mathbb{C}$ is an extension field of $\mathbb{Q}$. Since $\sqrt{3}$ is a zero of $x^2 - 3$, $\sqrt{3}$ is an algebraic element over $\mathbb{Q}$. Since i is a zero of $x^2 + 1$, i is also algebraic over $\mathbb{Q}$.

Ex. Although it's not that easy to prove, π and e are transcendental numbers over $\mathbb{Q}$.

Ex. Notice that π and e are transcendental over $\mathbb{Q}$ because there is no polynomial with coefficients in $\mathbb{Q}$ (or $\mathbb{Z}$) such that π or e is a solution to:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0; \qquad a_i \in \mathbb{Q} \text{ for all } i = 1, \dots, n.$$

However, π and e are algebraic over $\mathbb{R}$ because π is a root of $x - \pi = 0$ and e is a root of $x - e = 0$.

So whether a number is algebraic or transcendental can depend on which field you are taking it over.

Ex. Show $\sqrt{1+\sqrt{7}}$ is algebraic over $\mathbb{Q}$.

Let $\alpha = \sqrt{1+\sqrt{7}}$ then:

$$\alpha^2 = 1 + \sqrt{7}$$

$$\alpha^2 - 1 = \sqrt{7}$$

$$(\alpha^2 - 1)^2 = 7$$

$$\alpha^4 - 2\alpha^2 + 1 = 7 \text{ or } \alpha^4 - 2\alpha^2 - 6 = 0.$$

So α is a zero of $x^4 - 2x^2 - 6 = 0$ in $\mathbb{Q}[x]$ and α is algebraic over $\mathbb{Q}$.

Theorem: Let E be an extension field of F, and $\alpha \in E$, with α algebraic over F. Then there is an irreducible polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. $f(x)$ is uniquely determined up to a constant factor in F and is a polynomial of minimal degree ≥ 1 in $F[x]$ having α as a zero. If $g(\alpha) = 0$ for $g(x) \in F[x]$, with $g(x) \neq 0$, then $f(x)$ divides $g(x)$.

Ex. $x^2 - 2 = 0$, $3x^2 - 6 = 0$, and $x^3 - 2x = 0$ all have $\sqrt{2}$ as a zero.

Notice that $3x^2 - 6 = 3(x^2 - 2)$ and $x^3 - 2x = x(x^2 - 2)$.

$x^2 - 2$ and $3x^2 - 6$ are irreducible in $\mathbb{Q}[x]$ where $x^3 - 2x$ is not.

Def. Let E be an extension field of a field F, and let $\alpha \in E$ be algebraic over F. The unique **monic** polynomial (coefficient of the highest power is 1) $p(x)$, where $p(\alpha) = 0$ and $p(x)$ is irreducible over F, is the irreducible polynomial for α over F and will be denoted $\boldsymbol{irr(\alpha, F)}$**.** The degree of $irr(\alpha, F)$ is the degree of α over F, denoted by $\boldsymbol{deg(\alpha, F)}$**.**

Ex. We saw that $\alpha = \sqrt{1 + \sqrt{7}}$ is a zero of $x^4 - 2x^2 - 6$ in $\mathbb{Q}[x]$.

$x^4 - 2x^2 - 6$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$ since:

$$a_n = 1 \not\equiv 0\ (mod\ 2), \qquad -2 \equiv 0\ (mod\ 2)$$

$$-6 \equiv 0\ (mod\ 2) \quad \text{and} \quad -6 \not\equiv 0\ (mod(2^2)).$$

The leading coefficient is 1 so $irr\left(\sqrt{1 + \sqrt{7}}, \mathbb{Q}\right) = x^4 - 2x^2 - 6$, and $\deg\left(\left(\sqrt{1 + \sqrt{7}}\right), \mathbb{Q}\right) = 4$.

Ex. When we talk about the degree of an algebraic number, we must specify which field we are talking about. For example, for $\alpha = \sqrt{3}$:

$$irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \quad \text{so} \quad deg(\sqrt{3}, \mathbb{Q}) = 2,$$

$$\text{but } irr(\sqrt{3}, \mathbb{R}) = x - \sqrt{3} \quad \text{so} \quad deg(\sqrt{3}, \mathbb{R}) = 1.$$

Ex. Find $irr(\alpha, \mathbb{Q})$ and $deg(\alpha, \mathbb{Q})$ for $\alpha = \sqrt{3+i}$.

$$\alpha^2 = 3 + i$$

$$\alpha^2 - 3 = i$$

$$(\alpha^2 - 3)^2 = i^2 = -1$$

$$\alpha^4 - 6\alpha^2 + 9 = -1$$

$$\alpha^4 - 6\alpha^2 + 10 = 0.$$

So α satisfies $x^4 - 6x^2 + 10 = 0$.

$x^4 - 6x^2 + 10 = 0$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$ since: $a_4 = 1 \not\equiv 0 \ (mod\ 2)$, $-6 \equiv 0 \ (mod\ 2)$, and $10 \equiv 0 \ (mod\ 2)$, But $10 \not\equiv 0 \ (mod\ 2^2)$. So:

$$irr(\alpha, \mathbb{Q}) = x^4 - 6x^2 + 10, \qquad deg(\alpha, \mathbb{Q}) = 4.$$

Def. Suppose α is algebraic over F then $< irr(\alpha, F) >$ is a maximal ideal of $F[x]$. Therefore, $F[x]/< irr(\alpha, F) >$ is a field and is isomorphic to the image $\phi_\alpha\big[F[x]\big]$, where ϕ_α is the evaluation homomorphism. We call this field $\boldsymbol{F(\alpha)}$.

Def. An extension field E of a field F is a **simple extension** of F if $E = F(\alpha)$ for some $\alpha \in E$.

Theorem: Let E be a simple extension $F(\alpha)$ of a field F, and let α be algebraic over F. Let the degree of $irr(\alpha, F)$ be $n \geq 1$. Then every element γ of $E = F(\alpha)$ can be uniquely expressed in the form:

$$\gamma = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \text{ where } c_i \text{ are in } F.$$

Ex. $f(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$ because it is degree 2 and has no zero in $\mathbb{Z}_2$ since:

$$f(0) = 1 \text{ and } f(1) \equiv 1(mod\ 2).$$

By Kronecker's Theorem there exists an extension field E on $\mathbb{Z}_2$, which has a zero of $x^2 + x + 1$. By our previous theorem, elements of $E = \mathbb{Z}_2(\alpha)$ are of the form:

$$a_1\alpha + a_0 \quad \text{where} \quad a_0, a_1 \in \mathbb{Z}_2.$$

So the elements of $E = \mathbb{Z}_2(\alpha)$ are:

$$0 + 0\alpha = 0, \quad 1 + 0\alpha = 1, \quad 0 + 1\alpha = \alpha, \quad \text{and} \quad 1 + \alpha.$$

Thus $E = \mathbb{Z}_2(\alpha)$ is a finite field with 4 elements.

How do we add or multiply these elements? We need to use the fact that $\alpha^2 + \alpha + 1 = 0$ to do this. In $\mathbb{Z}_2$ we have:

$$\alpha^2 = -\alpha - 1 = \alpha + 1.$$

So, for example, if we want to multiply:

$$(\alpha)(1 + \alpha) = \alpha + \alpha^2 = \alpha + \alpha + 1 = 1.$$

So let's fill in the addition and multiplication tables for $\mathbb{Z}_2(\alpha)$:

$+$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\mathbf{1}+\boldsymbol{\alpha}$
$\mathbf{0}$	0	1	α	$1+\alpha$
$\mathbf{1}$	1	0	$1+\alpha$	α
$\boldsymbol{\alpha}$	α	$1+\alpha$	0	1
$\mathbf{1}+\boldsymbol{\alpha}$	$1+\alpha$	α	1	0

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\mathbf{1}+\boldsymbol{\alpha}$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Finally, let's show that $\mathbb{R}[x]/<x^2+1>\cong \mathbb{C}$:

$\mathbb{R}[\alpha] = \mathbb{R}[x]/<x^2+1>$ where elements of $\mathbb{R}(\alpha)$ are of the form:

$a_0 + a_1\alpha; \quad a_0, a_1 \in \mathbb{R}$ where $\alpha^2 = -1$.

We usually call $\alpha, \quad i = \sqrt{-1}$.

So $\mathbb{R}(\alpha) = \mathbb{R}[x]/<x^2+1> = \{a_0 + a_1\alpha |\, a_0, a_1 \in \mathbb{R},\ \alpha^2 = -1\}$

$\cong \{a + bi |\, a, b \in \mathbb{R},\ i = \sqrt{-1}\} = \mathbb{C}$.