Fields and Field Extensions

Recall: For ring theory in general, we tried to divide rings up into classes by looking at what happened with their ideals!

Unfortunately, this approach is completely hopeless for fields.

Theorem: (Simplicity) Every field K is a simple ring: the only ideals of K are K itself and $\{0_K\}$.

proof: Let I be an ideal of K and suppose $I \neq \{0_K\}$. Then $\exists\ x \in K$, $x \neq 0_K$. Since K is a field, x is a unit.

Therefore, x admits a multiplicative inverse x^{-1}.

Since I is an ideal,

$$1_K = x^{-1} \cdot x \in I.$$

Now since $1_K \in I$, if

$y \in K$, then

$$y = y \cdot 1_K \in I .$$

This shows $I = K$.

Observation: this proof shows that if R is a ring and I is an ideal of R containing a unit, then $I = R$.

Q: How to study fields? The previous theorem says they cannot be studied internally, so ...

A: Study fields externally! Starting with a field K, look at other fields that contain K.

Definition: (field extension) Let K be a field. A field L is called a **field extension** of K if $K \subseteq L$ (up to ring isomorphism) and K is a subring of L containing 1_L.

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

and let

$$L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ by setting $b = 0$.

$$1_L = 1 \in K = \mathbb{Q}.$$

We just need to show L is a field. We know $L \subseteq \mathbb{R}$ and the operations of $\mathbb{R}$ restrict to those of L.

We get that L is a commutative ring with unit. If $a+b\sqrt{2} \in L$, we know that if $a \neq 0 \neq b$, then the multiplicative inverse is $\dfrac{1}{a+b\sqrt{2}}$.

Why is this inverse in L?

Rationalize by multiplying by

$$1 = \frac{a-b\sqrt{2}}{a-b\sqrt{2}}$$

to get that the inverse is in L.

Therefore, $L = \mathbb{Q}(\sqrt{2})$ is a field extension of $\mathbb{Q}$.

Note: $\sqrt{2} \notin \mathbb{Q}$, so $L \neq \mathbb{Q}$.

Definition: (vector space) Let K be a field. A **vector space** over K is a set V endowed with two binary operations

vector addition "$+$" : $V \times V \to V$

Scalar multiplication "$\cdot$" : $K \times V \to V$

Such that

1) $(V, +)$ is an abelian group

2) $1_K \cdot x = x \quad \forall\, x \in V$

3) $\forall\ x, y \in V,\quad \alpha, \beta \in K,$

$$\alpha \cdot (x+y) = \alpha \cdot x + \alpha \cdot y$$

$$(\alpha+\beta) \cdot x = \alpha \cdot x + \beta \cdot x$$

(distributivity of "$\cdot$" over "$+$" and "$+$" over "$\cdot$")

4) $\forall\ \alpha, \beta \in K,\quad x \in V$

$$\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$$

(associativity)

Observation: (field extensions & vector spaces)

If K is a field and L is an extension field of K, then tracking through the definition, L is a vector space over K.

Everything holds since L is a field, so for example, 3) + 4) already hold for $\alpha, \beta \in L$, so in particular, for $\alpha, \beta \in K$.

Definition: (degree) The **degree** of an extension field L of a field K is just the dimension of L as a vector space over K:

$$\boxed{\deg(L/K) := \dim_K(L)}$$

where the dimension is the cardinality of a basis for L over K (scalars are elements of K).

Definition: (algebraic elements, extensions)

Let K be a field. Then $\alpha \in K$ is said to be **algebraic** over K if $\exists\ p(x) \in K[x]$ such that $p(\alpha) = 0_K$.

If α is not algebraic over K, we say α is **trascendental** over K.

Finally, an extension field L of K is said to be algebraic if every element of L is algebraic over K.

Example 2: ($\mathbb{C}$ over $\mathbb{R}, \mathbb{Q}$)

$\mathbb{C}$ is algebraic over $\mathbb{R}$

Since if $a+bi \in \mathbb{C}$

($a, b \in \mathbb{R}$), then consider

$$p(x) = (x-(a+bi))(x-(a-bi))$$

$$p(x) = x^2+a^2+b^2-2ax.$$

Then $p(a+bi) = 0$.

However, not even every element of $\mathbb{R}$ is algebraic over $\mathbb{Q}$: π and e are the most famous examples.

Observation: $\deg(\mathbb{C}/\mathbb{R}) = 2$

since $\{1, i\}$ is a basis

for $\mathbb{C}$ over $\mathbb{R}$.

$\deg(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = 2$

Since $\{1, \sqrt{2}\}$ is a basis

for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

But $\deg(\mathbb{R}/\mathbb{Q})$ is

infinite since $\mathbb{Q}$ is

countable, but $\mathbb{R}$ is not!

Any basis of $\mathbb{R}$ over $\mathbb{Q}$

must be magicked into existence

by the Axiom of Choice.

Definition: (algebraically closed) A field K is said to be **algebraically closed** if every non-constant polynomial in $K[x]$ has a root in K.

Immediate consequence: every polynomial in $K[x]$ for K algebraically closed factors linearly!

Lemma: Let k be a field. Then $k[x]$ is a principal ideal domain.

proof: We already proved that $k[x]$ has a division algorithm. So let I be an ideal in $k[x]$ and let $p(x) \neq 0$ be an element of minimal degree in I. Then if $f(x) \neq 0$, $f(x) \in I$, then by the division algorithm, $\exists$

$q(x), r(x) \in k[x]$

Such that

$$f(x) = q(x) \cdot p(x) + r(x)$$

with the degree of $r(x)$ less than the degree of $p(x)$.

But I is an ideal,

so $q(x) \cdot p(x) \in I$.

Therefore,

$$r(x) = f(x) - q(x) \cdot p(x) \in I.$$

But $p(x)$ has minimal degree in I, so $r(x) = 0$.

Therefore, $f(x) = q(x)\, p(x)$

$\Rightarrow I = \langle p(x) \rangle$. $\square$