date: thursday, march 21, 2024

Field Extensions I

Goal: Look at fields (special domains where all elements have inverses).

Standard Example: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ p a prime

Main problem: If F is a field and $p(x) \in F[x]$, can we find a "bigger" field so that $p(x)$ has a root in that field.

eg. x^2+1 is a polynomial in $\mathbb{R}[x]$. It has no root in $\mathbb{R}$ but if we make $\mathbb{R}$ "bigger" to make $\mathbb{C}$, then x^2+1 has a root (namely $i^2=-1$).

Extension Field

A field E is an extension of a field F if $E \supset F$ as a subfield. Call F the base field.

Note: Suppose we say E is an extension of F if E has a subfield F' such that $F \simeq F'$.

eg. $\mathbb{C}$ is an extension of $\mathbb{R}$

eg. $\mathbb{R}$ is an extension of $\mathbb{Q}$

Recall: If $p(x)$ is an irreducible polynomial in $F[x]$, then

$$F[x] / \langle p(x) \rangle$$

is a field. (Same if $\langle p(x) \rangle$ is a maximal ideal).

Gives a way to construct fields.

eg. x^2-2 in $\mathbb{Q}[x]$

Then, $\mathbb{Q}[x]/\langle x^2-2\rangle$ is a field.

Note: Contains a "copy" of $\mathbb{Q}$.

$$\{a+\langle x^2-2\rangle \mid a\in\mathbb{Q}\}\subseteq \mathbb{Q}[x]/\langle x^2-2\rangle$$

We have $\mathbb{Q}\simeq\{a+\langle x^2-2\rangle \mid a\in\mathbb{Q}\}$. So $\mathbb{Q}[x]/\langle x^2-2\rangle$ is an extension of $\mathbb{Q}$.

Observation: If $p(x)=a_0+a_1x+\cdots+a_nx^n\in F[x]$, we can view it as $p(x)=a_0(x)^0+a_1x^1+\cdots+a_nx^n$.

Let

$$\alpha=x+\langle x^2-2\rangle\in\mathbb{Q}[x]/\langle x^2-2\rangle.$$

Then,

$$\begin{aligned}\alpha^2-2(\alpha)^0 &= (x+\langle x^2-2\rangle)^2-2(x+\langle x^2-2\rangle)^0\\ &= (x^2+\langle x^2-2\rangle)-2(1+\langle x^2-2\rangle)\\ &= (x^2-2\cdot 1)+\langle x^2-2\rangle\\ &= 0+\langle x^2-2\rangle.\end{aligned}$$

So α is a root of x^2-2.

Fundamental Theorem of Field Theory

Let F be a field and $p(x)\in F[x]$ (with $p(x)$ not the constant polynomial). Then there exists an extension E of F such that $p(x)$ has a root $\alpha\in E$.

Proof

Since $F[x]$ is a PID, it's a UFD. So we can factor $p(x)=p_1(x)\cdots p_r(x)$ into irreducibles. It is enough to prove the result for $p_1(x)$ because it is irreducible.

$$E=F[x]/\langle p_1(x)\rangle$$

is a field.

Claim: E is a field.

First show (sketch) that E is an extension of F. Define a map $\varphi: F \to E$ by $a \mapsto a + \langle p(x) \rangle$. Check this is a ring homomorphism (you do this!) It is one-to-one since if

$$\varphi(a) = \varphi(b) \iff a + \langle p(x) \rangle = b + \langle p(x) \rangle$$
$$\iff a - b \in \langle p(x) \rangle$$

But $\deg p(x) \geq 1$ and $\deg a-b = 0$. So $a=b$. So $F \simeq \operatorname{Im}\varphi \subset E$.
Let $\alpha = x + \langle p(x) \rangle$ <— the class of x in E.
If $p_1(x) = a_n x^n + \cdots + a_1 x^1 + a_0 x^0$, then

$$\begin{aligned} p(\alpha) &= a_n \alpha^n + \cdots + a_1 \alpha^1 + a_0 \alpha^0 \\ &= a_n(x^n + \langle p(x) \rangle + \cdots + a_0(1 + \langle p(x) \rangle)) \\ &= (a_n x^n + \cdots + a_0) + \langle p(x) \rangle \\ &= 0 + \langle p(x) \rangle. \end{aligned}$$

So α is a root.

$\square$

Fact: If $p(x)$ is irreducible, the elements of $F[x]/\langle p(x) \rangle$ are in one-to-one correspondance with the set

$$\{r(x) \mid r(x) \in F[x] \text{ and } \deg r(x) < \deg p(x)\}.$$

To see why, let $g(x) + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$. By division algorithm,

$$g(x) = p(x)q(x) + r(x).$$

So

$$g(x) - r(x) = p(x)q(x) \in \langle p(x) \rangle.$$

So

$$g(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle.$$

Define a map,

$$F[x]/\langle p(x) \rangle \longrightarrow \{r(x) \mid \deg r(x) < \deg p(x)\}$$
$$g(x) + \langle p(x) \rangle \longmapsto r(x) \text{ where } g(x) = q(x)p(x) + r(x).$$

eg. What are the elements of $\mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$?

$x^2 + x + 1$ is irreducible since 0, 1 are not roots. So elements are in one-to-one correspondance with deg < 2 polynomials

$$\left.\begin{array}{ll} 0 & +\langle x^2+x+1\rangle \\ 1 & +\langle x^2+x+1\rangle \\ x & +\langle x^2+x+1\rangle \\ x+1 & +\langle x^2+x+1\rangle \end{array}\right\}\text{field with 4 elements}$$