Field Extensions

Example 1

Starting in $\mathbb{R}[x]$, let $p(x) = x^2 + 1$.

$p(x)$ is irreducible over $\mathbb{R}$. This follows from the fact that $p(x)$ has no roots in the real numbers.

Therefore, $S = \langle p(x) \rangle$ is maximal and so $F = \mathbb{R}[x]/S$ is a field

What are the elements of F? The easy answer is cosets of the form $a(x) + S$, but the persistent issue of nonuniqueness of coset generators remains.

Solution: Given a coset $a(x) + S$, generated by $a(x)$, we divide $a(x)$ by $p(x)$. Since the degree of $p(x)$ is 2, there are unique quotient and remainder. We focus on the remainder, $r(x) = r_0 + r_1 x$. Since $r(x)$ and $a(x)$ differ by a multiple of $p(x)$ and hence belongs to S, $a(x) + S = r(x) + S$.

To sum up, every element of F is a coset that contains a unique polynomial of the form $r_0 + r_1 x$. This is the representation of F we will use henceforth:

$$F = \{r_0 + r_1 \bar{x} \mid r_0,\ r_1 \in \mathbb{R}\}$$

The constant r_0 really stands for the coset $r_0 + S$ but the set $\{r_0 + S \mid r_0 \in \mathbb{R}\}$ is isomorphic to $\mathbb{R}$ (where $r_0 + S \mapsto r_0$)

The operation on F, is still the operation on cosets, so to add or multiply elements of F, we perform the usual operations on polynomials over the real numbers, but to identify the coset that is the result, we must then divide by $p(x)$ and retain only the remainder.

For addition, this is simplified by the fact that the sum of polynomials of degree one or less will have a degree one or less. Therefore the division step isn't necessary. Therefore,

$$(r_0 + r_1 \bar{x}) + (s_0 + s_1 \bar{x}) = (r_0 + s_0) + (r_1 + s_1)\bar{x}$$

Multiplication is a bit more involved. To compute $(r_0 + r_1 \bar{x})(s_0 + s_1 \bar{x}$ you first multiply:

$$(r_0 + r_1 \bar{x})(s_0 + s_1 \bar{x}) = r_1 s_1 \bar{x}^2 + (r_1 s_0 + r_0 s_1)\bar{x} + r_0 s_0$$

We list the terms of the product in descending order of degree because we will be dividing by $p(\bar{x}) = \bar{x}^2 + 1$:

$$\begin{array}{ll}
 & \quad r_1 s_1 \\
\bar{x}^2 + 1 & \overline{)\, r_1 s_1 \bar{x}^2 + (r_1 s_0 + r_0 s_1)\bar{x} + r_0 s_0} \\
 & \underline{r_1 s_1 \bar{x}^2 + \qquad\qquad\qquad\qquad r_1 s_1} \\
 & \quad (r_1 s_0 + r_0 s_1)\bar{x} + (r_0 s_0 - r_1 s_1)
\end{array}$$

Therefore, $(r_0 + r_1 \bar{x})(s_0 + s_1 \bar{x}) = (r_0 s_0 - r_1 s_1) + (r_1 s_0 + r_0 s_1)\bar{x}$

We already know that F must be field, but let's look at multiplicative inverses:

$(r_0 + r_1 \bar{x})^{-1} = (s_0 + s_1 \bar{x})$ if

$(r_0 + r_1 \bar{x})(s_0 + s_1 \bar{x}) = 1 + 0\bar{x}$

or

$(r_0 s_0 - r_1 s_1) + (r_1 s_0 + r_0 s_1)\bar{x} = 1 + 0\bar{x}$

or

$r_0 s_0 - r_1 s_1 = 1$

$r_1 s_0 + r_0 s_1 = 0$

Remember, we assume r_0 and r_1 are given, so the two equations above are linear equations which can be put into matrix form:

$$\begin{pmatrix} r_0 & -r_1 \\ r_1 & r_0 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

There is a unique solution to this system if and only if the determinant of the matrix of coefficients is nonzero.

$$\begin{vmatrix} r_0 & -r_1 \\ r_1 & r_0 \end{vmatrix} = {r_0}^2 + {r_1}^2$$

Therefore, only the zero of F has no multiplicative inverse, which is what we expect.

The field F is called the splitting field for $p(x)$ because $p(x)$ factors into linear factors over F:

$$p(\bar{x}) = \bar{x}^2 + 1 = -1 + 1 = 0 \Rightarrow x - \bar{x} \text{ is a factor of } p(x)$$

Dividing $x - \bar{x}$ into $p(x)$, we get $p(x) = (x - \bar{x})(x + \bar{x})$

The field we have just constructed is isomorphic to the complex numbers. To see this, we define $\psi : \mathbb{R}[x] \to \mathbb{C}$ where $\psi(a(x)) = a(i)$. It can be proven that ψ is a homomorphism with kernel $S = \langle p(x) \rangle$. Therefore, the First Isomorphism Theorem tells us that $F = \mathbb{R}[x]/S \approx \psi(\mathbb{R}[x]) = \mathbb{C}$.

Example 2

Start in $\mathbb{Q}[x]$ and consider $p(x) = x^2 - 2$ and construct $\mathbb{Q}\left(\sqrt{2}\right)$

Example 3

Start in $\mathbb{Z}_3[x]$ and consider $p(x) = x^2 + x + 2$ and construct GF(9), the unique field of order 9.

```
In[165]:= rules3 = {α^k_ /; k ≥ 2 :> Expand[α^(k-2) (2 α + 1), Modulus → 3]};
In[166]:= reduce3[a_] := Expand[a //. rules3, Modulus → 3]
In[167]:= {#, reduce3[α^#]} & /@ Range[1, 8]
```

Out[167]=

$$\begin{pmatrix} 1 & \alpha \\ 2 & 2\alpha + 1 \\ 3 & 2\alpha + 2 \\ 4 & 2 \\ 5 & 2\alpha \\ 6 & \alpha + 2 \\ 7 & \alpha + 1 \\ 8 & 1 \end{pmatrix}$$

Example 4

Start in $\mathbb{Z}_2[x]$ and consider $p(x) = x^3 + x + 1$ and construct GF(8), the unique field of order 8.

```
In[159]:= rules4 = {β^k_ /; k ≥ 3 :> Expand[β^(k-3) (β + 1), Modulus → 2]};
In[160]:= reduce4[a_] := Expand[a //. rules4, Modulus → 2]
```

In[161]:=
```
{#, reduce4[β^#]} & /@ Range[1, 7]
```

Out[161]=

$$\begin{pmatrix} 1 & \beta \\ 2 & \beta^2 \\ 3 & \beta + 1 \\ 4 & \beta^2 + \beta \\ 5 & \beta^2 + \beta + 1 \\ 6 & \beta^2 + 1 \\ 7 & 1 \end{pmatrix}$$