Math 521A

5.3 – The Structure of $F[x]/(p(x))$ When $p(x)$ is Irreducible

Theorem (Theorem 5.10)

Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then the following statements are equivalent:

(1) *$p(x)$ is irreducible in $F[x]$.*

(2) *$F[x]/(p(x))$ is a field.*

(3) *$F[x]/(p(x))$ is an integral domain.*

The proof (worked out on the board) is carried out by showing that:

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1).$$

The part $(2) \Rightarrow (3)$ is immediate once you recall that every field is an integral domain (see Theorem 3.8, p. 66). □

Recall that $F[x]/(p(x))$ *always* contains F as a subring. In particular, if $p(x)$ is irreducible, $F[x]/(p(x))$ is a field which contains F a subfield:

$F[x]/(p(x))$ is called an extension field of F.

- Let p be a positive prime. An extension field E of the finite field $\mathbb{Z}_p$ can be obtained by choosing an irreducible polynomial $f(x)$ of degree k over F. Then $E = F[x]/(f(x))$ and $|E| = p^k$.
- It is possible to show that *any* finite field is isomorphic to an extension of $\mathbb{Z}_p$ for some positive prime p.
- Finite fields are denoted by $\mathrm{GF}(p^k)$. GF stands for Galois Field. Évariste Galois (1811–1832), shown below, was the French mathematician who discovered them. These fields are the building blocks of cryptographic systems currently in use (AES, elliptic-curve cryptosystems, etc.), and error-correcting schemes (Reed-Solomon codes) used in CDs, DVDs, and Blu-ray discs.

Theorem (Theorem 5.11)

Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. Then $F[x]/(p(x))$ is an extension field of F that contains a root of $p(x)$.

Example

Let $F = \mathbb{Z}_2$ and $p(x) = x^3 + x + 1$ be an irreducible polynomial in $F[x]$. $p(x)$ has no roots in F. Consider

$$R = \frac{F[x]}{(p(x))} = \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$$

where $\alpha = [x] \in R$ is such that $\alpha^3 + \alpha + 1 = [x^3 + x + 1] = [0]$, i.e., $\alpha \in R$ is a root of $p(x) \in F[x]$.

Example

Although the last example may seem artificial, you have done a similar procedure when you "accepted" the existence of complex numbers. For this, consider $p(x) = x^2 + 1 \in \mathbb{R}[x]$. $p(x)$ has no roots in $\mathbb{R}$, but it does so in a field containing $\mathbb{R}$, namely, $\mathbb{C}$. Construct the ring $R = \frac{\mathbb{R}[x]}{(p(x))}$ and show that $p(x)$ has a root $\alpha = [x]$ in there.

Example

Determine addition and multiplication rules in the field of the previous example, i.e., determine formulas for $(a + b\alpha) + (c + d\alpha)$ and $(a + b\alpha)(c + d\alpha)$ for all $a, b, c, d \in \mathbb{R}$.

Corollary (Corollary 5.12)

Let F be a field and $f(x)$ a nonconstant polynomial in $F[x]$. Then there is an extension field K of F that contains a root of $f(x)$.