Galois Theory

Robert F. Coleman

Lecturte 4

Last Time

We used the fact that $F[x]$ is a PID when we proved

Proposition. *If F is a field and $g(x) \in F[x]$ is irreducible of positive degree d then $E =: F[x]/(g(x))$ is a extension field of the image of F (which is isomorphic to F) of degree d.*

Theorem. *If $F \subseteq L \subseteq E$, then $[E : F] = [E : L] \cdot [L : F]$.*

Proof.

$\mathbf{Q}$ is the only proper subfield of $\mathbf{Q}[x]/(x^3 - 2)$.

An element $\alpha \in E$ such that $f(\alpha) = 0$ for some non-zero $f \in F[x]$ is said to be **algebraic over** F. If $A \subseteq E$, $F(A)$ is smallest extension of F in E containing A.

Proposition. *An element $\alpha \in E$ is algebraic over F iff $[F(\alpha) : F] < \infty$.*

Proof.

Lemma. *Any subring of E containing and finite dimensional over F is a field.*

Proof.

One calls $[F(\alpha) : F]$ the degree of α over F.

Theorem. *The set L of elements in E algebraic over F is a field extension of F.*

Proof. $F \subseteq L$.

Suppose $\alpha, \beta \in L$. Let $a_1, \ldots, a_n$ be a basis for $F(\alpha)$ and $b_1, \ldots, b_m$ be a basis for $F(\beta)$. Then $\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ spans $F(\alpha, \beta)$.

Suppose $\alpha \in E$ is algebraic over F.
Let $I = \{f \in f[x] : f(\alpha) = 0\}$. The monic polynomial $g_\alpha(x)$ such that $I = (g_\alpha(x))$ is called the minimal polynomial of α.

Lemma. $\deg g_\alpha(x) = \deg(\alpha)$.

Proof.

Corollary. *There are no extensions of* $\mathbf{R}$ *of finite odd degree.*

Proof.

Homework for Monday

Read §4.4-§4.7.

Do exercises 4.5-4.7