

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Definition: Let E/F be a field extension, $\alpha \in E$ algebraic over F . Consider the surjective ring homomorphism: $\phi : F[x] \rightarrow F[\alpha]$ defined $f(x) \mapsto f(\alpha)$. Let $\ker \phi = (h(x))$ where $h(x)$ is a monic irreducible polynomial in $F[x]$ such that $h(\alpha) = 0$. $h(x)$ is called the minimal polynomial of α over F , and is denoted $\text{Irr}(\alpha, F)$.

Remarks:

- h is uniquely defined, since if $(h_1) = (h_2)$ then $h_1 \mid h_2$ and $h_2 \mid h_1$ so $h_1 = h_2$ since they are monic.
- $F[\alpha] \cong F[x]/(h(x))$
- h is a nonzero polynomial of smallest degree of which α is a root.

Theorem: Let α be algebraic over F . Then $[F(\alpha) : F] = \deg \text{Irr}(\alpha, F)$.

Proof: Let $h(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 = \text{Irr}(\alpha, F)$. I claim that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an F -basis for $F(\alpha)$. Indeed, let us show linear independence first. Suppose that $d_0 \cdot 1 + d_1\alpha + \dots + d_{n-1}\alpha^{n-1} = 0$. Then α is a root of $g(x) = d_0 + d_1x + \dots + d_{n-1}x^{n-1} \in F[x]$. But $\deg g(x) < \deg(h(x))$, hence $g(x) = 0$. So $d_0 = d_1 = \dots = d_{n-1} = 0$. To show spanning, note that as α is algebraic, $F(\alpha) = F[\alpha]$. So, it is enough to show that $\alpha^i \in \text{span}_F\{1, \alpha, \dots, \alpha^{n-1}\}$. Induct on i with the cases $i \leq n-1$ being obvious. So, supposing that $\alpha^i \in \text{span}\{1, \alpha, \dots, \alpha_n\}$ and writing down the expression for α^i then multiplying by α^{j+1} give you the result.

Definition: Let E/F be a field extension. E/F is **finite** if $[E : F] < \infty$ and E/F is **finitely generated** if E is finitely generated as a field over F (i.e. $E = F(\alpha_1, \dots, \alpha_n)$). E/F is **algebraic** provided α is algebraic over F for all $\alpha \in E$.

Theorem: Let E/F be a field extension. Then E/F is finite $\Leftrightarrow E/F$ is finitely generated and algebraic.

Proof: " \Rightarrow ": Let $\alpha_1, \dots, \alpha_n$ be an F -basis for E . Then $E = F\alpha_1 + F\alpha_2 + \dots + F\alpha_n \subseteq F(\alpha_1, \dots, \alpha_n) \subseteq E$. Therefore, $E = F(\alpha_1, \dots, \alpha_n)$, hence we have that E/F is finitely generated. To show that E/F is algebraic, let $\alpha \in E$. Then $F \subseteq F(\alpha) \subseteq E$. So we have that $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ where $[E : F]$ is finite. Therefore $[F(\alpha) : F] < \infty$, therefore by a previous theorem, α is algebraic over F .

" \Leftarrow ": Let $E = F(\alpha_1, \dots, \alpha_n)$, and in general, set $L_i = F(\alpha_1, \dots, \alpha_i)$. Then we have a tower of fields and we can use the fact about multiplicativity of field extensions to get that $[E : F] < \infty$.

Corollary: Suppose that $\alpha_1, \dots, \alpha_n$ are algebraic over F and let $p(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$. Then $p(\alpha_1, \dots, \alpha_n)$ and $\frac{1}{p(\alpha_1, \dots, \alpha_n)}$ are algebraic, since both are in $F(\alpha_1, \dots, \alpha_n)$.

Theorem (recall from 817-818): Eisenstein's Criterion for Irreducibility: Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ be a polynomial in $\mathbb{Z}[x]$. Suppose that there exists a prime p such that $p \mid a^i$ for $i \leq n-1$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over \mathbb{Q} .

Gauss's Lemma: Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x) = h(x)g(x)$ where $h(x), g(x) \in \mathbb{Q}[x]$, where $\deg h > 0$ and $\deg g > 0$. Then $\exists h_1(x), g_1(x) \in \mathbb{Z}[x]$ such that $f(x) = h_1(x)g_1(x)$, $h_1 = \alpha h$ and $g_1 = \beta g$ for some $\alpha, \beta \in \mathbb{Q}$.

Corollary: Let E/F be a field extension. Set $L := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$. Then L is a field by our previous work. L is often called the algebraic closure of F in E .

Example: $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$. Show that $\bar{\mathbb{Q}}$ is algebraic but not finite. Indeed, suppose that $[\bar{\mathbb{Q}} : \mathbb{Q}] = n$ and consider $\sqrt[n+1]{2}$. We know that $\text{Irr}(\sqrt[n+1]{2}, \mathbb{Q}) = x^{n+1} - 2$ since that polynomial is irreducible over \mathbb{Q} by Eisenstein. So the degree of the field extension is $n+1$ which we know has to divide n , a contradiction.

Proposition: Let $f(x) \in F[x]$ with degree $f \geq 2$ or 3 . Then $f(x)$ is reducible $\Leftrightarrow f(x)$ has a root in $F[x]$.

The Mod p technique: Let $f \in \mathbb{Z}[x]$, and suppose \exists a prime p such that p doesn't divide the leading coefficient of f and $f(x) \in \mathbb{Z}_p[x]$ is irreducible. Then f is irreducible in \mathbb{Q} .

Example: