Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Theorem/Definition: Let F be a field. Then TFAE:

1. If E/F is an algebraic field extension, then $E = F$.
2. Every nonconstant polynomial in F splits completely in $F[x]$.
3. Every nonconstant polynomial in $F[x]$ has a root in F.

If F satisfies any of the three equivalent definitions above, then F is said to be **algebraically closed**.
Proof: (1) $\Rightarrow$ (2): Let $f(x) \in F[x]$ and let E be the splitting field of $f(x)$ over F. Then E/F is algebraic, so by (1), $E = F$ hence $f(x)$ splits completely in $F[x]$.

(2) $\Rightarrow$ (3) is trivial.

(3) $\Rightarrow$ (1) Let E/F be an algebraic field extension. Let $\alpha \in E$. Let $f(x) = \text{Irr}(\alpha, F)$. By (3), $f(x)$ has a root in F, so $\deg f = 1$ and therefore $f(x) = x - \alpha$. Therefore, $\alpha \in F$ and so $E = F$.

Definition: Let F be a field. A field E containing F is an algebraic closure of F if E/F is algebraic and E is algebraically closed.

Proposition: Suppose L/F is a field extension and L is algebraically closed. Let $E = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$. Then E is an algebraic closure of F in L.
Proof: We have show that E is a field and that E/F is algebraic. It is hence enough to show that E is algebraically closed. Suppose $f(x)$ in $E[x]$ is a nonconstant polynomial. Then $f(x) \in L[x]$, so $f(x)$ has a root $\alpha \in L$. Threfore α is algebraic over E, as $f(\alpha) = 0$. So, $E(\alpha)/E$ is an algebraic extension, but E/F is algebraic, so that $E(\alpha)/F$ is algebraic. Thus α is algebraic over F, so $\alpha \in E$, by definition of E. So E is algebraically closed since we proved condition (3) of the above definition.

Lemma: Let K be a field. Then $\exists$ a field L containing K such that every nonconstant polynomial in $K[x]$ as a root in L.
Proof: For each nonconstant polynomial $f(x) \in K[x]$ let x_f be a new variable. Let $R = K[\{x_f \mid f \in K[x] \setminus K\}]$. Let I be the ideal generated by $\{f(x_f)\}$.

Claim: $I \neq R$. If $I = R$, then $1 \in I$ which means $1 = \sum_{i=1}^n r_i f_i(x_{f_i})$ for some $r_i \in R$. So, the r_i's involve only finitely many of the variables. Let $x_i = x_{f_i}$, and let $x_{n+1}, \ldots, x_m$ be all the other variables appearing in the r_i. Threfore, we have that

$$1 = \sum_{i=1}^n r_i(x_1, \ldots, x_m) f_i(x_i).$$

Now, let F be a splitting field for $f_1(x)f_2(x)\cdots f_n(x)$ over K, i.e. in F, every $f_i(x)$ has a root α_i. Certainly the above equation still holds in $F[\{x_f\}]$. Now, let $x_i = \alpha_i$ for $i = 1, \ldots, n.$; Then the above equation after substituting reads $1 = 0$, a contradiction. So, I is a proper ideal. Then by the previous proposition, there exists a maximal ideal $\mathfrak{m}$ of R that contains I. Let $L = R/\mathfrak{m}$, which is a field. Note that the composition of maps, call it δ, below:

$$K \hookrightarrow K[\{x_f\}] \to K[\{x_f\}]/\mathfrak{m}$$

is 1-1 as $\mathfrak{m}$ has no units. So, we identify K with $\delta(K)$ in L and consider $K \subset L$. Let $f(x) \in K[x] \setminus K$. Let $\alpha_f = x_f + \mathfrak{m}$. Then $f(\alpha_f) = f(x_f + \mathfrak{m}) = f(x_f) + \mathfrak{m}$. But $f(x_f) \in I \subseteq \mathfrak{m}$ so $f(\alpha_f) = \bar{0}$, as desired.

Theorem: Let F be a field. Then there exists an algebraic closure of F.
Proof: We can construct by the previous lemma a chain of fields:

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$$

where every nonconstant polynomial in $L_n[x]$ has a root in L_{n+1}. Let $L = \bigcup_{n\geq 0} L_n$. Note that L is a field. I claim that L is algebraically closed. Indeed, let $f(x) \in L[x] \setminus L$. Then there exists an n such that $f(x) \in L_n[x]$. Then f has a root in L_{n+1} with is also in L. So, by the theorem, $\{\alpha \in L \mid \alpha$ is algebraic over $F\}$ is an algebraic closure of F and this completes the proof.

Theorem: Let E/F be an algebraic extension and L/K an extension in which L is an algebraic closure of K. Let $\sigma : F \to K$ be a nonzero field homomorphism. Then there exists a field map $\tau : E \to L$ that extends σ.
Proof: We will use Zorn's Lemma. Let $\Lambda = \{(T, \phi) \mid F \subset T \subset E$ and $\phi : T \to L$ extends $\sigma\}$. Partially order Λ as follows: $(T_1, \phi_1) \leq (T_2, \phi_2) \;\Leftrightarrow\; T_1 \subset T_2$ and $\phi_2|_{T_1} = \phi_1$. First, note that $\Lambda \neq \emptyset$ as $(F, \sigma) \in \Lambda$. Let C be a totally ordered subset of Λ. Let $T_0 \bigcup_{(T,\phi)\in C} T$ and define $\psi : T_0 \to L$ as follows. Let $t \in T_0$. Then $t \in (T_1, \phi_1) \in C$. Define $\psi(t) = \phi(t)$. By the extension part of the condition of being in Λ this is well-defined. It is easy to check that ψ is a field homomorphism.
Then $(T_0, \psi) \in \Lambda$ and is an upper bound for C. By Zorn's Lemma, Λ has a maximal element, call it (M, δ). It is enough to show that $M = E$. Suppose that $M \subsetneq E$. Let $N = \delta(M)$. Then $\delta : M \to N$ is a field isomorphism. So, let $\alpha \in E \setminus M$. Then α is algebraic over M as E is algebraic over F. Let $f(x) = \mathrm{Irr}(\alpha, M)$. Then $M(\alpha) \cong M[x]/(f(x)) \cong N[x]/(f^\delta(x))$. But $f^\delta(x) \in N[x] \subset L[x]$ has a root $\beta \in L$ as L is algebraically closed. So, $N[x]/(f^\delta(x)) \cong N(\beta)$, since $f^\delta(x)$ is irreducible over N. Nut $N(\beta) \subset L$. Let $\delta' : M(\alpha) \hookrightarrow L$ be the composition of the maps above. By construction, $\delta'|_M = \delta$. Hence, $(M(\alpha, \delta') \supsetneq (M, \delta)$, a contradiction. Therefore, $M = E$.

Corollary: Let F be a field and E_1, E_2 two algebraic closures of F. Then there exists an isomorphism $\tau : E_1 \to E_2$ such that τ fixes F.
Proof: Let $\sigma : F \to F$ be the identity map. Then there exists $\tau : E_1 \to E_2$ such that $\tau|_F = \mathrm{Id}_F$. As E_1 is algebraically closed, so is $\tau(E_1)$. But $E_2/\tau(E_1)$ is algebraic, so $E_2 = \tau(E_1)$, so the map is surjective, hence an isomorphism.

Definition: Let F be a field and S a set of polynomials in $F[x]$. The splitting field L for S over F is the smallest subfield of $\bar{F}$(the algebraic closure of F), such that every polynomial in S splits completely in this field. I.e. $L = F$(all roots in $\bar{F}$ of all polynomials in S).

Remark: Let E/F and L/F be field extensions and $\sigma : E \to L$ a field map that fixes F. Suppose that $p(x) \in F[x]$ has a root $\alpha \in E$. Then $\sigma(\alpha)$ is also a root of $p(x)$.
Proof: Let $p(x) = c_n x^n + \cdots + c_1 x + c_0 \in F[x]$. So, we know that $0 = c_n \alpha^n + \cdots + c_1 \alpha c_0$. Applying σ to both sides gives $0 = c_n \sigma(\alpha)^n + \cdots + c_1 \sigma(\alpha) + c_0$ since σ is a homomorphsim and also fixes F. Therefore $\sigma(\alpha)$ is a root of $p(x)$.

Proposition: Let E/F be an algebraic extension and $\sigma : E \to E$ a field map which fixes F. Then σ is surjective and hence an automorphism of E.
Proof: Let $\beta \in E$. Let $p(x) = \mathrm{Irr}(\beta, E)$. Let $\{\beta_1, \ldots, \beta_t\}$ be the roots of $p(x)$ which lie in E, and wlog, let $\beta_1 = \beta$. By the remark, $\sigma(\beta_i)$ is also a root for all i and hence in E. Therefore $\sigma : \{\beta_1, \ldots, \beta_t\} \to$

$\{\beta_1, \ldots, \beta_t\}$ is an injective set map, and hence is also onto. In particular, $\sigma(\beta_i) = \beta_i = \beta$ for some β_i above. Hence $\beta \in \text{im}(\sigma)$.

Theorem/Definition: Let E/F be an algebraic extension. Then TFAE:

1. E is the splitting field for some set of nonconstant polynomials in $F[x]$
2. Every irreducible polynomial in $F[x]$ which has a root in E splits in E.
3. If $\sigma : E \to \bar{F}$ is a field map that fixes F, then $\sigma(E) = E$ (i.e. σ is really an automorphism of E.

If E/F satisfies (1),(2),or (3) then E/F is called a **normal** extension.
Proof: (2) $\Rightarrow$ (1): Let $\alpha \in E$, and let $p_\alpha(x) = \text{Irr}(\alpha, F)$. By (2), $p_\alpha(x)$ splits in E. Let $S = \{p_\alpha(x) \mid \alpha \in E\}$. Then E is the splitting field for S.
(1) $\Rightarrow$ (3): Let $\sigma : E \to \bar{F}$ be an embedding fixing F. We need to show that $\sigma(E) = E$. As E/F is algebraic, and by the proposition, we need only show that $\sigma(E) \subseteq E$. By (1), E is the splitting field for a set $S \subseteq F[x] \setminus F$. Therefore, $E = F$(all roots of all polynomials in S). Let β be a root of $p(x) \in S$. Since σ fixes F, $\sigma(\beta)$ is also a root of $p(x)$. But $p(x)$ splits in E, therefore $\sigma(\beta) \in E$, hence $\sigma(E) \subseteq E$.
(3) $\Rightarrow$ (2): Let $p(x)$ be an irreducible polynomial in $F[x]$ which has a root $\alpha \in E$. Let $\beta \in \bar{F}$ be any root of $p(x)$. Let τ the composition of the maps:

$$F(\alpha) \to F[x]/(p(x)) \to F(\beta)$$

$$\alpha \to x + (p) \to \beta$$

Therefore, $\tau : F(\alpha) \to F(\beta)$ is an isomorphism that sends α to β and fixes F. By an old theorem, we can extend $\tau : E \to \bar{F}$. By (3), $\sigma(E) = E$, therefore $\beta = \sigma(\alpha) \in E$. Therefore $p(x)$ splits in E.

Remarks/Examples:

1. If $[E : F] = 2$, then E/F is normal. Indeed, pick $\alpha \in E \setminus F$. Certainly $E = F(\alpha)$. Let $f(x) = \text{Irr}(\alpha, F)$. Then $(x - \alpha)$ is a factor of $f(x)$, so $f(x) = (x - \alpha)(x - \beta)$ for some $\beta \in E$. Then E is the splitting field for $f(x)$.
2. Take $E = \mathbb{Q}(\sqrt[3]{2})$. Then $x^3 - 2$ has a root in E, but $x^3 - 2$ doesn't split in E because its other roots are not real, and $E \subset \mathbb{R}$. So $E/\mathbb{Q}$ is not normal.
3. Recall that if $K \subseteq F \subseteq E$, then E/K is algebraic $\Leftrightarrow$ E/F and F/K is algebraic. The same does not occur in the normal case. Suppose that $K \subseteq F \subseteq E$ and E/K is normal. Then E/F is normal, but F/K need not necessarily normal. For a counterexample, let L be the splitting field for $x^3 - 2$ over $\mathbb{Q}$, and take E to be in the above example. Then $L/\mathbb{Q}$ is normal by definition, and hence L/E is normal. However, $E/\mathbb{Q}$ is not normal.
4. Suppose that E/K is finite. Then E/K is normal $\Leftrightarrow$ E is the splitting field over K of a single polynomial. For the forward direction, suppose that $E = K(\alpha_1, \ldots, \alpha_n)$, let $f_i(x) = \text{Irr}(\alpha_i, K)$. Then E is the splitting field for $f(x) = f_1(x) \cdots f_n(x)$. The reverse direction is by definition.
5. Let $\{L_i\}$ be a collection of fields, all of which are normal over F a field. Then $\bigcap L_i$ is normal over F.

Definition: Let E/F be an algebraic extension. Then the **normal closure** of E/F is the smallest field $L \supseteq E$ such that L/F is normal. Just let $L = \bigcap K$ where $E \subseteq K \subseteq \bar{F}$ and K/F is normal. Clearly L is normal over F by the previous remark and is contained in any normal extension of F containing E by definition.

Example: Let $E = \mathbb{Q}(\sqrt[3]{2})$, and $F = \mathbb{Q}$. We saw last time that E/F is not normal. The normal closure of E/F is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. It is normal as it is the splitting field for $x^3 - 2$. It is the closure because suppose that $L/\mathbb{Q}$ is normal and $L \subseteq \mathbb{Q}(\sqrt[3]{2})$. Then $x^3 - 2$ has a root in L and L is normal, so $x^3 - 2$ splits in L, therefore L contains ω. So, $L \supseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ and therefore $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the normal closure of E/F. Along these lines, we have the following useful proposition:

Proposition: Suppose that $E = F(\alpha_1, \ldots, \alpha_n)$, and suppose that E/F is algebraic. Let $f_i(x) = \mathrm{Irr}(\alpha_i, F)$. Let L be the splitting field for $f(x) = f_1(x) \cdots f_n(x)$ over F. Then L is the normal closure of E/F.

Proof: L/F is normal as it is the splitting field of $f(x)$. If $T \supseteq E$ and T/F is normal, then $f_i(x)$ has a root in T and hence splits in T for all i. Therefore, $T \subseteq L$. So, L is the smallest normal extension of F containing E. For another example, let $E = \mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{3})$. Then the normal closure of $E/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[5]{2}, e^{2\pi i/5}, \sqrt[3]{3}, e^{2\pi i/3})$.