

Frank Moore
 Algebra 901 Notes
 Professor: Tom Marley

Definition: Let R be a commutative ring with identity. Then R is a **field** provided every nonzero element of R is a unit.

Definition: R is a **domain** if whenever $ab = 0$, then $a = 0$ or $b = 0$.

Definition: If R is a domain then the **quotient field** or **field of fractions** of R is $Q(R) := \{\frac{a}{b} \mid a, b \in R, b \neq 0\}$. Note that $Q(R)$ is a field and is the smallest field containing R .

Definition: $R[x_1, \dots, x_n] :=$ the polynomial ring in n variables with coefficients from R . Note that we may think of $R[x_1, \dots, x_n]$ as $R[x_1, \dots, x_{n-1}][x_n]$.

Notation/Definition: Suppose $R \subseteq S$, where R, S are commutative rings with 1. Let $\alpha_1, \dots, \alpha_n \in S$. Then $R[\alpha_1, \dots, \alpha_n] := \bigcap T$ where $R \subset T \subset S$ and $\alpha_1, \dots, \alpha_n \in T$. In other words, it is the smallest ring containing R and $\alpha_1, \dots, \alpha_n$. Another way to describe it is as follows:

$$R[\alpha_1, \dots, \alpha_n] = \{p(\alpha_1, \dots, \alpha_n) \mid p(x_1, \dots, x_n) \in R[x_1, \dots, x_n]\}$$

Definition: Let $F \subset E$ be fields. We say that E/F is a field extension. Let $\alpha_1, \dots, \alpha_n \in E$. With the above notation, we note that $F[\alpha_1, \dots, \alpha_n]$ is the smallest ring containing F and the α_i and is in fact a domain. We also make the following definition:

$$F(\alpha_1, \dots, \alpha_n) := \bigcap L$$

where $F \subseteq L \subseteq E$ is a field and $\alpha_i \in L$ for all i . This is the quotient field of L and we may also describe $F(\alpha_1, \dots, \alpha_n)$ as follows:

$$F(\alpha_1, \dots, \alpha_n) := \left\{ \frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)} \mid p, q \in F[x_1, \dots, x_n], q(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

Note that the above is the smallest field containing F and the α_i .

Definition: Let E/F be a field extension. Then E can be considered a vector space over F . The degree (E/F) is defined to be the dimension of E as an F -vector space. Notation: $[E : F] = \dim_F E$.

Lemma: Let E/F and F/L be field extensions. Then $[E : L] = [E : F][F : L]$.

Proof: Suppose $\{\alpha_1, \dots, \alpha_m\}$ is an F -basis for E and $\{\beta_1, \dots, \beta_l\}$ is an L -basis for F . Then $\{\alpha_i \beta_j\}$ where $1 \leq i \leq m$ and $1 \leq j \leq l$ is an L -basis for E .

Definition: Let E/F be a field extension and let $\alpha \in E$. Then α is **algebraic** over F if α is a root of a nonzero polynomial in $F[x]$. Otherwise, α is **transcendental** over F . In fact, we may choose the above polynomial to be monic by dividing by the leading coefficient.

Theorem: Let E/F be a field extension and $\alpha \in E$. Then TFAE:

1. α is algebraic over F .

2. $F[\alpha] = F(\alpha)$.
3. $[F(\alpha) : F]$ is finite.

Proof:

- 1) \Rightarrow 2): Note that $F[\alpha] = \text{span}_F\{1, \alpha, \alpha^2, \dots\}$. Consider the ring homomorphism: $\phi : F[x] \rightarrow F[\alpha]$ given by $f(x) \mapsto f(\alpha)$. Note by our remarks above, ϕ is surjective. As α is algebraic, we know that $\ker \phi \neq 0$. As $\ker \phi$ is an ideal, and $F[x]$ is a PID, we get that $\ker \phi = (h(x))$ for some $h \in F[x]$ where we may take h to be monic. Therefore, we have that $F[\alpha] \cong F[x]/(h(x))$. Note that $F[\alpha]$ has no zerodivisors as it is a subring of a field. Therefore, $F[x]/(h(x))$ has no ZD so that h is irreducible. Therefore, $(h(x))$ is a maximal ideal of $F[x]$ so $F[\alpha]$ is a field, hence $F[\alpha] = F(\alpha)$.
- 2) \Rightarrow 3): As $\frac{1}{\alpha} \in F(\alpha) = F[\alpha]$, $\frac{1}{\alpha} = c_0 + c_1\alpha + \dots + c_n\alpha^n$ for some n with $c_n \neq 0$. Therefore, we have that

$$c_n\alpha^{n+1} + c_{n-1}\alpha^n + \dots + c_1\alpha^2 + c_0\alpha - 1 = 0$$

and hence

$$\alpha^{n+1} = \left(-\frac{c_{n-1}}{c_n}\right)\alpha^n + \left(-\frac{c_{n-2}}{c_n}\right)\alpha^{n-1} + \dots + \frac{1}{c_n}$$

I claim that $F[\alpha] = \text{span}_F\{1, \dots, \alpha^n\}$. Indeed, it is enough to show that $\alpha^i \in \text{span}_F\{1, \alpha, \dots, \alpha^n\}$ for all i . We proceed by induction on i . If $i \leq n$ then the result follows. So, suppose we know that $\alpha_j \in \text{span}_F\{1, \alpha, \dots, \alpha^n\}$. Then α^{j+1} is just α times the expression for α^j in terms of our basis so using the above formula for α^{n+1} we get the desired result. Therefore, we have that $[F(\alpha) : F] = \dim_F F(\alpha) = \dim_F F[\alpha] \leq n + 1$ so that $[F(\alpha) : F] < \infty$ as desired.

- 3) \Rightarrow 1): Suppose that $[F(\alpha) : F] = n$. Consider $S = \{1, \alpha, \dots, \alpha^n\}$. Then S is linearly dependent over F . Then there exists c_0, \dots, c_n not all zero such that

$$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$$

Thus α is a root of $d(x) = c_0 + c_1x + \dots + c_nx^n$ which is nonzero because c_0, \dots, c_n were not all zero. So α is algebraic.