

1 Field Extensions I

Definition 1 (Integral domain). Let R be a commutative ring. Then R is an integral domain if $ab = 0$ implies that $a = 0$ or $b = 0$ for all $a, b \in R$.

Definition 2 (Euclidean domain). Let R be an integral domain. Then R is a Euclidean domain if there exists some function $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that for all $a, b \neq 0 \in R$, there exist elements $q, r \in R$ such that $a = qb + r$ where $r = 0$ or $f(r) < f(b)$.

Theorem 1.1 (Bézout's Identity). Let R be a Euclidean domain. For $a, b \in R$, there exists $\alpha, \beta \in R$ such that $\gcd(a, b) = \alpha a + \beta b$.

Definition 3 (Irreducible). Let F be a field, and $f \in F[t] \setminus F$. Then f is irreducible if $\nexists g, h \in F[t] \setminus F$ of strictly smaller degree such that $f = gh$.

Definition 4 (Unique factorization domain). Let R be an integral domain. Then R is a unique factorization domain (UFD) if for irreducible $p_i \in R$, any nonzero $x \in R$ can be written uniquely (up to ordering) as $x = p_1 p_2 \cdots p_k$, $k \geq 1$.

Fact: If R is an Euclidean domain, then R is a UFD (and PID)

Corollary 1. Let $f \in \mathbb{F}[t]$ be a monic polynomial with $\deg f \geq 1$. Then we can write $f = f_1 f_2 \cdots f_k$ uniquely (up to ordering) for irreducible monic polynomials f_j .

Definition 5. Let R be a UFD. When $a_0, \dots, a_n \in R$ are not all 0, we can generalize the greatest common divisor of a_0, \dots, a_n (written $\gcd(a_0, \dots, a_n)$) any element $c \in R$ satisfying

- (i) $c \mid a_i$ ($0 \leq i \leq n$), and
- (ii) if $d \mid a_i$ ($0 \leq i \leq n$), then $d \mid c$.

When $f = \sum_{j=0}^d a_j x^j \in R[x]$ is a non-zero polynomial, we define a content of f to be any $\gcd(a_0, \dots, a_d)$ and $\gcd(f) = \gcd(a_0, \dots, a_d)$. We say that $f \in R[X]$ is primitive if $f \neq 0$ and the content of f is divisible only by units of R .

Lemma 1.2 (Gauss). $\gcd(fg) = \gcd f \cdot \gcd g$

Corollary 2. $f \in \mathbb{Z}[t]$ is irreducible $\iff f$ is irreducible over $\mathbb{Q}[t]$

Corollary 3. If R is a UFD with field of fractions Q and $f \in R[X]$ with $\deg f > 0$, then f is irreducible in $R[X]$ $\iff f$ is irreducible in Q .

Theorem 1.3 (Eisenstein's Criterion). Let R be a UFD with field of fractions Q and let $f = a_0 + a_1 X + \dots + a_n X^n \in R[X]$ with $\gcd(f) = 1$. Suppose there exists an irreducible element $p \in R$ such that

- (i) $p \mid a_i$ for $0 \leq i < n$,
- (ii) $p^2 \nmid a_0$, and
- (iii) $p \nmid a_n$,

then f is irreducible in $R[X]$ (and hence also in $Q[X]$).

Definition 6 (Field extension). Let L and K be fields. Then L is an extension of K if there exists a homomorphism $\varphi : K \rightarrow L$. Then we write $L : K$ or L/K , $\varphi(K) \cong K$ and identify $\varphi(K)$ with K .

Fact: Suppose that L is a field extension of K with associated embedding $\varphi : K \rightarrow L$. Then L forms a vector space over K , under the operations

$$\begin{aligned} \text{(vector addition)} \quad \psi : L \times L &\rightarrow L & \text{given by} \quad (v_1, v_2) &\mapsto v_1 + v_2 \\ \text{(scalar multiplication)} \quad \tau : K \times L &\rightarrow L & \text{given by} \quad (k, v) &\mapsto \varphi(k)v. \end{aligned}$$

Definition 7 (Degree, finite extension). Let $L : K$. Then the degree of $L : K$ is $[L : K] = \dim L$ over K as a vector space. We say that $L : K$ is a finite extension if $[L : K] < \infty$.

Definition 8 (Tower, intermediate field). We say that $M : L : K$ is a tower of field extensions if $M : L$ and $L : K$ are field extensions, and in this case we say that L is an intermediate field (relative to the extension $M : K$)

Theorem 1.4 (The Tower Law). *Suppose that $M : L : K$ is a tower of field extensions. Then $M : K$ is a field extension, and $[M : K] = [M : L][L : K]$.*

Corollary 4. *Suppose that $L : K$ is a field extension for which $[L : K]$ is a prime number. Then whenever $L : M : K$ is a tower of field extensions with $K \subseteq M \subseteq L$, one has either $M = L$ or $M = K$.*