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 $f : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ 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 $x = p_1 p_2 \cdots p_k, \quad k \geq 1$.*

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

Corollary 1.2. *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 $a_0, \ldots, a_n \in R$ are not all 0, we can generalize the greatest common divisor of $a_0, \ldots, a_n$ (written gcd($a_0, \ldots, a_n$)) 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 $f = a_0 + a_1 X + \ldots + a_n X^n$ is a non-zero polynomial in $R[X]$, we define a content of f to be any $\gcd(a_0, \ldots, a_n)$. 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 1.3 (Gauss). *Suppose that R is a UFD with field of fractions Q. Suppose that f is a primitive element of $R[X]$ with $\deg f > 0$. Then f is irreducible in $R[X]$ if and only if f is irreducible in Q.*

Theorem 1.4 (Eisenstein's Criterion). *Suppose that R is a UFD, and that $f = a_0 + a_1 X + \ldots + a_n X^n \in R[X]$ is primitive. Then provided that there is an irreducible element p of R having the property 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 $Q[X]$, where Q is the field of fractions of R.

Definition 6 (Field extension). *When K and L are fields, we say that L is an extension of K if there is a homomorphism $\varphi : K \to L$. Then $\varphi(K) \cong K$ and we write $L : K$ or L/K.*

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

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

Definition 7 (Degree, finite extension). *Suppose that $L : K$ is a field extension. We define the degree of $L : K$ to be the dimension of L as a vector space over K. We use the notation $[L : K]$ to denote the degree of $L : K$. Further, 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 1.5 (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 1.6. *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 $M = K$.*