Contents

Chapter I

Modules

1 Basics

March 24, 2023

Theorem 1.1. *Any two bases of a free modules over an integral domain are in bijection.*

2 Cyclic modules over PIDs

March 23, 2023

Convention. *All the modules from now on (except in appendices) will be over PIDs unless stated otherwise.*

R will denote a generic PID, and M an R-module.

Definition 2.1 (Cyclic submodule)**.** A module that can be generated by a single element is called cyclic.

Proposition 2.2. *Any submodule of a cyclic module is cyclic.*

Definition 2.3 (Order)**.** Annihilator of an $m \in M$ is any $a \in A$ such that[1]

$$\operatorname{Ann}(m) = (a).$$

[1] We define annihilators of a subset (not just submodules!) of M in the obvious manner.

Notation. *Perversely, we denote a generic order (which will be unique up to associates!) of* m*, by* $|m|$.

Whenever we use them in the statements a result, we will mean that $|m|$ *is an arbitrary order of* m.

Proposition 2.4. *Let* $m \in M$ *and* $a \in A \setminus 0$. *Then*[2]

$$|am| \sim \frac{|m|}{\gcd(a, |m|)}$$

where $\sim$ *is the "being associates" relation.*

[2]Note that the "a/b" notation makes sense only in integral domains.

Chapter II

Field extensions

1 Characteristic and field homomorphisms

April 7, 2023

Convention. *Throughout this chapter, F, K, L will be reserved for fields.*

Definition 1.1 (Field characteristic)**.** Let ϕ be the unique nice ring homomorphism on $\mathbb{Z} \to F$. Then we define $\operatorname{char} F$ to be the unique nonnegative integer p such that $\ker \phi = (p)$.

Corollary 1.2. *Characteristic of a field is either 0 or a prime integer.*

Definition 1.3 (Field homomorphisms and isomorphisms)**.** A field homomorphism (respectively isomorphism) is a nice ring homomorphism (respectively isomorphism) between fields.

Corollary 1.4. *Field homomorphisms are injective.*

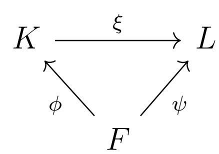
2 Field extensions

April 7, 2023

Definition 2.1 (F-extensions)**.** A field homomorphism $f\colon F \to K$ is called an F-extension.

Remark. *When the context is clear, we'll let K stand in place of f.*

Definition 2.2 (F-extension homomorphisms)**.** Let $\phi\colon F \to K$ and $\psi\colon F \to L$ be field extensions and $\xi\colon K \to L$ a field homomorphism (respectively isomorphism). Then (ϕ, ξ, ψ) is called an F-extension homomorphism (respectively isomorphism) iff the following diagram commutes:



Remark. *When the context is clear, we'll let ξ stand for (ϕ, ξ, ψ).*

Definition 2.3 (Degree of field extensions)**.** Let $\phi\colon F \to K$ be an extension. Then ϕ is an algebra, and the dimension of K as the vector space over F is called ϕ's *degree*, and is denoted $[K : F]_\phi$.

Depending on the degree, we call the extension *finite* or *infinite*.

Proposition 2.4. *Degree of isomorphic F-extensions coincide.*

Proposition 2.5 (Degree is multiplicative)**.** *For extensions $F \xrightarrow{\phi} K \xrightarrow{\psi} L$, we have that*

$$[L : F]_{\psi\circ\phi} = [L : K]_\psi \, [K : F]_\phi.$$

3 Simple extensions

April 7, 2023

Definition 3.1 (Simple extensions)**.** An extension $\phi\colon F \to K$ is called simple iff

$$K = \phi(F)(\alpha)$$

for some $\alpha \in K$.

Notation. *Given a ring homomorphism $\phi\colon A \to B$, we'll denote by $f \mapsto f_\phi$ the induced homomorphism $A[x] \to B[x]$.*

Theorem 3.2 (Extensions via irreducible polynomials)**.** *Let $p \in F[x]$ be irreducible.*[1] *Let ϕ be the composite of the canonical maps:*

$$F \longrightarrow F[x] \longrightarrow F[x]/(p), \qquad \phi\colon F \dashrightarrow F[x]/(p)$$

Then ϕ is an extension of degree $n := \deg p$ with[2] *$(\overline{x}^0, \ldots, \overline{x}^{n-1})$ being a basis. We also have that*

$$F[x]/(p) = \phi(F)[\overline{x}] = \phi(F)(\overline{x})$$

with "p having a root in $F[x]/(p)$", namely $\overline{x}$:

$$p_\phi(\overline{x}) = 0$$

Definition 3.3 (Algebraics and transcendentals)**.** Let $\phi\colon F \to K$ be an extension and $\alpha \in K$. Let $\psi\colon F[x] \to \phi(F)[\alpha]$ be the evaluation at α via ϕ. Then we call α *ϕ-algebraic* iff $\ker \psi \neq 0$, and *ϕ-transcendental* otherwise.

We call ϕ an *algebraic extension* iff each element of K is ϕ-algebraic.

Remark. *Again, if clear from the context, we'll drop "ϕ-".*

Definition 3.4 (Minimal polynomials)**.** Continuing Definition 3.3, and assuming that α is ϕ-algebraic, we call the unique monic polynomial p that generates $\ker \psi$, the ϕ-minimal polynomial of α.

Proposition 3.5. *Continuing Definition 3.3, we have the following:*

(i) If α is algebraic, then its minimal polynomial p is irreducible and $\phi(F)(\alpha) = \phi(F)[\alpha] \cong F[x]/(p)$.

(ii) If α is transcendental, then $\phi(F)(\alpha) \cong F(x)$.

Proposition 3.6 (On non-simple algebraic extensions)**.** *Let $\phi\colon F \to K$ be an extension and $\alpha_1, \ldots, \alpha_n \in K$ for $n \geq 0$. Let $L := \phi(F)(\alpha_1, \ldots, \alpha_n)$. Then the following are equivalent:*

(i) ϕ as $F \to L$ is algebraic.

(ii) Each α_i is ϕ-algebraic.

---

[1] Since F is a field, this means that p is nonconstant.

[2] Since 1_F present, we can use the "x^i" notation.

(iii) $[L : F]_\phi < \infty$.[3]

If the above equivalent conditions hold, then we have that

$$\phi(F)(\alpha_1, \ldots, \alpha_n) = \phi(F)[\alpha_1, \ldots, \alpha_n].$$

4 Splitting extensions

April 26, 2023

Definition 4.1 (Splitting extension)**.** An extension $\phi\colon F \to K$ is called splitting for a polynomial $f \in F[x] \setminus \{0\}$ iff

(i) $f_\phi = c(x - \alpha_1)\cdots(x - \alpha_n)$ for $n \geq 0$ in $K[x]$; and

(ii) $K = \phi(F)(\alpha_1, \ldots, \alpha_n)$.

Theorem 4.2 (Existence)**.** *Each nonzero polynomial has a splitting extension.*

Theorem 4.3 (Isomorphism extension)**.** *Let $\mu\colon F_1 \to F_2$ be an isomorphism. Let $\phi_1\colon F_1 \to K_1$ be a splitting extension for $f \in F[x] \setminus \{0\}$ and $\phi_2\colon F_2 \to K_2$ be one for f_μ. Then there exists an isomorphism $\nu\colon K_1 \to K_2$ making the following commute:*

$$\begin{array}{ccc} F_1 & \xrightarrow{\mu} & F_2 \\ {\scriptstyle \phi_1}\downarrow & & \downarrow{\scriptstyle \phi_2} \\ K_1 & \xrightarrow[\nu]{} & K_2 \end{array}$$

Corollary 4.4. *Any two splitting field extensions of an $f \in F[x] \setminus \{0\}$ are F-extension isomorphic.*

5 Algebraic closures

Do this!

[3] The ϕ is actually a restriction.

6 Separable extensions

April 26, 2023

Definition 6.1 (Separable polynomials and extensions)**.** An *irreducible polynomial* $f \in F[x]$ is called separable iff it[4] has no repeated roots in any of (equivalently, one of) its splitting extensions.[5]

A *polynomial* $f \in F[x] \setminus \{0\}$ is called separable iff all of its irreducible factors are separable.

An *algebraic extension* $\phi\colon F \to K$ is called separable iff the minimal polynomial of each $\alpha \in K$ is separable.

Proposition 6.2 (The formal derivative)**.** *Define* $D_F\colon F[x] \to F[x]$ *by*

$$\sum_{i=0}^{n} a_i\, x^i \mapsto \sum_{i=1}^{n} n a_i\, x^{i-1}.$$

Then the following hold:

(i) D *is linear.*

(ii) For $f, g \in F[x]$, *we have*

$$D_F(fg) = D_F(f)\, g + f\, D_F(g).$$

(iii) If $\phi\colon F \to K$ *is a homomorphism, then*

$$D_K \circ \phi = \phi \circ D_F.$$

Notation. *We'll often use the more convenient notation of* f'.

Lemma 6.3 (Extensions preserve gcd's of polynomials)**.** *Let* $\phi\colon F \to K$ *be an extension and* $S \subseteq F[x]$ *with* $d \in F[x]$ *being a* gcd. *Then* d_ϕ *is a* gcd *of* $\phi(S)$.

Proposition 6.4 (Characterizing separability)**.** *Let* $f \in F[x] \setminus \{0\}$. *Then the following are equivalent:*

(i) f *is separable.*

[4]By "it", we obviously mean f_ϕ.

[5]Equivalently, f has no repeated roots in any of (not *some* of) its extensions.

(ii) f, f' *have no common zero in any extension.*[6]

(iii) f, f' *have a unit as their* gcd *in some (equivalently, in all) extensions.*

Corollary 6.5. *The (nonzero) polynomials of a field with characteristic* 0 *are always separable.*

Example 6.6 (A class of non-separable polynomials)**.** If $\operatorname{char} F = p > 0$, then any nonconstant polynomial in

$$F[x^p] := \left\{ \text{polynomials of the form } \sum_{i=0}^{n} a_i\, x^{pi} \right\}$$

is non-separable.

[6] Of course, we mean the *images* of f and f'.

Chapter III

Galois theory

1 The set Aut_ϕ

April 26, 2023

Corollary 1.1 (Group of field-fixing automorphisms)**.** *Given an extension $\phi\colon F \to K$, the set*

$$\mathrm{Aut}_\phi := \{F\text{-extension isomorphisms } K \to K\}$$

forms a group under function composition.

Remark. *If one wants to be more explicit than necessary for the benefit of clarity, they might write $\mathrm{Aut}_{\phi(F)}(K)$.*

Corollary 1.2. *Given the extensions $F \xrightarrow{\phi} K \xrightarrow{\psi} L$, we have that*

$$\mathrm{Aut}_\psi \leq \mathrm{Aut}_{\psi\circ\phi}\,.$$

Proposition 1.3 (The fixed subfield)**.** *Given an extension $\phi\colon F \to K$ and a subset $H \subseteq \mathrm{Aut}_\phi$, the set*

$$\mathrm{Fix}_\phi(H) := \{\text{elements of } K \text{ that remain fixed by all } \sigma \in H\}$$

forms a subfield of K containing $\phi(F)$.

Also, if $H_1 \subseteq H_2$, then $\mathrm{Fix}_\phi(H_1) \supseteq \mathrm{Fix}_\phi(H_2)$.

Lemma 1.4. *Let $\phi\colon F \to K$ and $\psi\colon F \to L$ be isomorphic F-extensions. Then as groups,*

$$\mathrm{Aut}_\phi \cong \mathrm{Aut}_\psi\,.$$

2 Galois groups

April 26, 2023

Definition 2.1 (Galois groups)**.** The group Aut_ϕ is called a Galois group of $f \in F[x]$ iff ϕ is a splitting extension of f.

Remark. *The Galois groups of f are unique up to isomorphisms.*

Lemma 2.2 ("Roots get mapped to roots")**.** *Consider the following F-extension homomorphism:*

$$\begin{array}{ccc} & F & \\ {\scriptstyle\phi}\swarrow & & \searrow{\scriptstyle\psi} \\ K & \xrightarrow[\xi]{} & L \end{array}$$

Then for any $f \in F[x]$, we have

$$f_\phi(\alpha) = 0 \text{ in } K \implies f_\psi(\xi(\alpha)) = 0 \text{ in } L.$$

Theorem 2.3. *Let $\phi\colon F \to K$ be splitting for $f \in F[x] \setminus \{0\}$. Then*

$$|\mathrm{Aut}_\phi| \leq [K : F]_\phi$$

with equality holding for separable f's.

3 Galois extensions

April 26, 2023

Definition 3.1 (Galois extensions)**.** An extension $\phi\colon F \to K$ is called Galois iff

$$|\mathrm{Aut}_\phi| = [K : F]_\phi < \infty.$$

Example 3.2 ($\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2}, \omega)$)**.** *Do this!*

Notation. *By F^*, we'll mean the multiplicative group of F.*

Definition 3.3 (Characters of groups)**.** A character of a group G is a group homomorphism $G \to F^*$.

Example 3.4. A field extension $F \to K$ induces a character $F^* \to K^*$.

Proposition 3.5 ("Linear independence" of characters of a group)**.** *Let* $\chi_1, \ldots, \chi_n \colon G \to F^*$ *be characters of a group* G *for* $n \geq 0$ *and* $\alpha_1, \ldots, \alpha_n \in F$. *Then*

$$\alpha_1 \chi_1 + \cdots + \alpha_n \chi_n = 0 \implies \text{each } \alpha_i = 0.$$

Appendix A

Some ring theory

1 Having zero and identity

April 4, 2023

Definition 1.1 (Notions in commutative rings)**.** On a *commutative ring*, we can define the following:

(i) "$a \mid b$" and "$a \sim b$" relations.

(ii) gcd, lcm of subsets.

(iii) prime elements.

If the ring also has an *identity*, then we can also define irreducibles.

If the ring is further an integral domain, then we also have "a/b" whenever $b \mid a$ and $a \neq 0$.

Remark. *We may also call irreducibles as* atoms *occasionally.*

Proposition 1.2 (Facts for commutative rings)**.** *In a commutative ring, the following hold:*

(i) $a \sim b$ *and* $c \sim d \implies ac \sim bd$.

(ii) Let d *be a* gcd *of* S. *Then* d' *is also a* gcd *of* $S \iff d \sim d'$. *Similarly for* lcm.

(iii) p *is prime* $\iff (p)$ *is nonzero prime.*

(iv) $\sim$ *preserves primality.*

Proposition 1.3 (When we also have an identity)**.** *In a commutative ring with identity, the following hold:*

(i) $\sim$ *becomes an equivalence relation.*

(ii) $\sim$ *preserves irreducibility.*

(iii) (p) *is maximal and nonzero* $\implies$ p *is irreducible.*[1]

(iv) Maximal ideals are prime.

(v) "$a \mid b$*" becomes a "partial order" with "= replaced with* $\sim$*".*

(vi) *(a)* $\sum_{s\in S}(s) = (d) \implies d$ *is a* gcd *of* S.
(b) $\bigcap_{s\in S}(s) = (m) \implies m$ *is an* lcm *of* S.

Remark. *We'll occasionally call integral domains simply as domains.*

Proposition 1.4 (When we have no zero divisors)**.** *In an integral domain, the following hold:*

(i) $a \sim b \iff a = ub$ *for some unit* u.

(ii) nd *is a* gcd *of* nS *and* $n \neq 0 \implies d$ *is a* gcd *of* S. *The converse holds if* nS *has a* gcd. *Similarly for* lcm.

(iii) Let $a, b \neq 0$. *Then the following hold:*

(a) d *is a* gcd *of* a, b *and* ax, bx *have* gcd*'s for each* $x \implies ab/d$ *is an* lcm *of* a, b.

(b) m *is an* lcm *of* a, $b \implies ab/m$ *is a* gcd *of* a, b.

(iv) Primes are irreducible.

(v) "Uniqueness" of prime factorizations.[2]

(vi) Form of divisors of prime products.[3]

(vii) Any two prime products have a gcd.

2 Euclidean domains

April 4, 2023

[1]Converse holds in Bézout domains. See Corollary 6.4.

[2]This comes in two versions: (i) "$p_1 \cdots p_m = q_1 \cdots q_n$" form; and (ii) "$up_1^{e_1} \cdots p_m^{e_m} = vq_1^{f_1} \cdots q_n^{f_n}$" form. In the latter, p_i's (respectively q_j's) need to be nonassociates.

[3]This also comes in two versions. However, we don't need p_i's to be nonassociates here in either version.

Definition 2.1 (Euclidean domains)**.** Let D be a domain. Then a *primitive Euclidean valuation* on D is a function $\nu\colon D \setminus \{0\} \to \mathbb{N}$ such that for every $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that the following hold:

(i) $a = bq + r$.

(ii) $r \neq 0 \implies \nu(r) < \nu(b)$.

ν is called a *Euclidean valuation* iff it also satisfies

$$\nu(ab) \leq \nu(a)\,\nu(b).$$

A domain with a Euclidean valuation is called a Euclidean domain.

Proposition 2.2 (Euclidean valuations from primitive)**.** *Let D be a domain with a primitive Euclidean valuation ν. Then D becomes a Euclidean domain with the following valuation:*

$$a \mapsto \min_{x \neq 0} \nu(ax) \qquad (a \neq 0)$$

Corollary 2.3. *Let D be a Euclidean domain with valuation ν. Then the following hold:*

(i) The minimum value of ν is $\nu(1_D)$.

(ii) $a \mid b \implies \nu(a) \leq \nu(b)$ for $a, b \neq 0$.

(iii) $a \sim b \implies \nu(a) = \nu(b)$ for $a, b \neq 0$.

(iv) u is a unit $\iff \nu(u) = \nu(1_D)$.

Proposition 2.4. *A Euclidean domain is a PID.*

3 GCD and LCM domains

April 5, 2023

Definition 3.1 (GCD and LCM domains)**.** A domain in which finite sets have gcd's (respectively lcm's) are called GCD (respectively LCM) domains.

Corollary 3.2. *PID's are GCD domains.*

Corollary 3.3. *A sufficient condition for a domain to be a GCD (respectively LCM) domain is that any two elements have a* gcd *(respectively an* lcm*).*

Corollary 3.4. *A GCD domain is an LCM domain, and conversely.*

Result 3.5. Let D be a domain and p be a nonprime atom. Therefore, take a, b such that $p \mid ab$ but $p \nmid a, b$. Then ab and pb don't have any $\gcd$. Consequently, the ideal (ab, pb) is not principal either.

Example 3.6 (A Noetherian domain that is not GCD)**.** 2 is a nonprime atom in the Noetherian $\mathbb{Z}[\sqrt{-3}]$, dividing

$$4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

but neither of the factors.[4]

Corollary 3.7. *In a GCD domain, irreducibles and primes coincide.*

4 Atomic domains

April 4, 2023

Definition 4.1 (Atomic domains)**.** A domain in which every nonzero nonunit admits an irreducible factorization.

Corollary 4.2. *Any nonzero element of an atomic domain admits a factorization of the form*

$$u\, p_1^{e_1} \cdots p_n^{e_n}$$

for $n \geq 0$, where u is a unit, p_i's are non-associate irreducibles and each $e_i \geq 1$.

Definition 4.3 (Ascending chain condition on principal ideals, ACCP)**.** An arbitrary ring is said to satisfy ACCP iff every ascending chain of its principal ideals stabilizes.

Definition 4.4 (Well-founded relations)**.** A relation R on a set X is called well-founded iff every nonempty subset of X has a minimal element.

Corollary 4.5. *In a domain, ACCP is equivalent to having that the "proper" divisibility is well-founded.*[5]

Theorem 4.6. *An domain satisfying ACCP is atomic.*

Corollary 4.7. *Noetherian domains are atomic.*[6]

[4] Note that $\mathbb{Z}[\sqrt{-3}]$ is Noetherian (and hence atomic; see Theorem 4.6), being the image of the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-3}]$.

[5] Requires DC.

[6] Converse not true; see Example 5.3.

5 Unique factorization domains

April 5, 2023

Definition 5.1 (UFD's)**.** An atomic domain in which each irreducible factorization is "unique".

Example 5.2 (A Noetherian domain that is not a UFD)**.** In $\mathbb{Z}[\sqrt{-5}]$,

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

are irreducible factorizations with $2 \not\sim 1 \pm \sqrt{-5}$.

Example 5.3 (A UFD that is not Noetherian)**.** $\mathbb{Z}[x_1, x_2, \ldots]$.[7]

Theorem 5.4. *For a domain D, the following are equivalent:*[8]

(i) D satisfies ACCP and its irreducibles are prime.

(ii) D is a UFD.

(iii) D is atomic as well as a GCD domain.

Corollary 5.5. *PID's are UFD's.*

Example 5.6 (A UFD that is not a PID)**.** In the UFD $\mathbb{Z}[x, y]$, the ideal $(2, x)$ is not principal.[9]

6 Bézout domains

April 5, 2023

Definition 6.1 (Bézout domains)**.** A domain in which each finitely generated ideal is principal.

Corollary 6.2 (Relation with gcd's)**.** *Let A be a commutative ring with identity and $a_1, \ldots, a_n \in A$. Then the following are equivalent:*

---

[7] That it's a UFD will follow from This will follow from Theorem 7.7.

[8] Do (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii).

[9] That this is a UFD follows from Theorem 7.7.

(i) *a_i's have a* gcd *of the form* $a_1x_1 + \cdots + a_nx_n$.

(ii) $(a_1, \ldots, a_n)$ *is principal.*

Proposition 6.3 (Relation with Bézout lemma)**.** *For a domain D, the following are equivalent:*

(i) *D is Bézout.*

(ii) *D is GCD; and, whenever d is a* gcd *of a, b, we have*

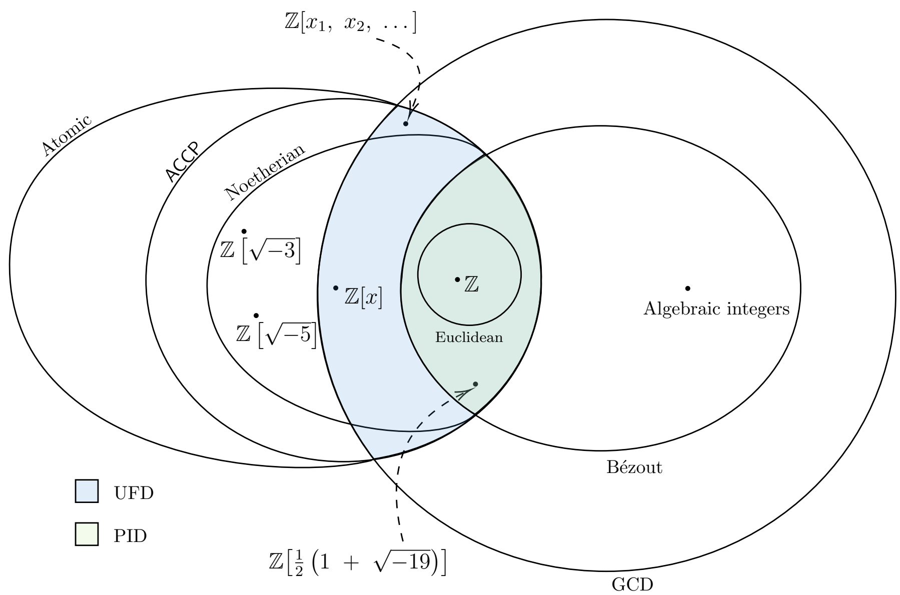
$$(d) = (a) + (b).$$

Corollary 6.4. *In a Bézout domain, irreducibles form maximal ideals.*

Corollary 6.5. *PID $\implies$ Bézout $\implies$ GCD.*

Theorem 6.6. *Bézout + ACCP $\implies$ PID.*

Proposition 6.7 (Nice summary)**.** *We have the following Venn diagram:*[10]



In particular, we have the following implications:

$$\begin{array}{ccccc} & & \text{UFD} & & \\ & \nearrow & & \searrow & \\ \text{Euclidean} \implies \text{PID} & & & & \text{GCD} \\ & \searrow & & \nearrow & \\ & & \text{Bézout} & & \end{array}$$

[10]Each portion is nonempty.

Not yet proven the above for algebraic integers and $\mathbb{Z}[(1+\sqrt{-19})/2]$!

7 Studying polynomial rings

April 5, 2023

Convention. *In this section A will denote a commutative ring with identity, unless otherwise stated.*

Definition 7.1 (Primitives and very primitives)**.** A polynomial f in $A[x_1, \ldots, x_n]$ is called *very primitive*[11] iff the A-ideal generated by its coefficients is the entire A.

f is called *primitive* iff 1_A is a gcd of the coefficients of f.

Convention. *We'll identity the common elements of A, $A[x]$, $A[x, y]$, etc.*

Theorem 7.2. *Let $f, g \in A[x_1, \ldots, x_n]$. Write $f = \sum_{|\alpha| \leq m} a_\alpha x^\alpha \in A[x_1, \ldots, x_n]$ for $m, n \geq 0$. Then the following hold:*

(i) f is a unit $\iff$ a_0 is a unit and all the rest are nilpotents.

(ii) f is a nilpotent $\iff$ each a_α is a nilpotent.

(iii) An ideal of $A[x_1, \ldots, x_n]$ which is annihilated by some nonzero polynomial is also annihilated by some nonzero constant.[12]

(iv) fg is very primitive $\iff$ f, g are very primitive.

(v) fg is primitive $\implies$ f, g are primitive.[13]

Theorem 7.3 (Eisenstein)**.** *Let $\mathfrak{p}$ be a prime ideal of A. Let $f := \sum_{i=0}^{n} a_i x^i \in A[x]$ such that the following hold:*

(i) $a_0, \ldots, a_{n-1} \in \mathfrak{p}$ but $a_n \notin \mathfrak{p}$.

(ii) $a_0 \notin \mathfrak{p}^2$.

Then we can't write f as a product of two polynomials each having strictly smaller degree.[14]

---

[11] Following Paolo's terminology.
[12] This is due to Conrad.
[13] See Theorem 7.4 for a converse.
[14] The hypotheses automatically imply that $f \neq 0$, so that we can talk of its degree.

Theorem 7.4 (Gauss' lemma)**.** *Let D be a GCD domain wherein each nonunit has an irreducible (or equivalently, prime) factor. Then the following hold:*

(i) f, g *in* $D[x]$ *are primitive* $\implies$ fg *is primitive.*

(ii) Irreducibles of $D[x]$ *are also irreducible in* $\mathrm{Frac}(D)[x]$.

Lemma 7.5 (Irreducibles and primitives)**.**

(i) Nonconstant irreducibles polynomials over a GCD domain are primitive.

(ii) A nonconstant primitive polynomial over a domain that doesn't factor into two polynomials of strictly smaller degrees, is primitive.

Lemma 7.6. *Primitive polynomials over a domain admit irreducible factorizations.*

Theorem 7.7. *D is a UFD* $\implies$ $D[x_1, \ldots, x_n]$ *is a UFD.*

Corollary 7.8. *D is a UFD* $\implies$ $D[x_1, x_2, \ldots]$ *is a UFD.*