Dummit & Foote § 7.1

13 a) $n = a^k b \Rightarrow n \mid (ab)^{k+1} = ab^k \cdot a^k b$

$\Rightarrow \overline{ab}^{k+1} = \overline{0}$ en $\mathbb{Z}/n\mathbb{Z}$

$\Rightarrow \overline{ab}$ is nilpotent

b) $n = q_1 \cdots q_r$, where $q_i = p_i^{n_i}$

$\Rightarrow n \mid (a p_1 \cdots p_r)^{\max(n_1, \dots, n_r)}$

$\Rightarrow a p_1 \cdots p_r$ is nilpotent

On the other hand,

$p_i \nmid m \Rightarrow p_i \nmid m^k \Rightarrow n \nmid m^k$

$\Rightarrow m^k$ is not nilpotent

Hence $\mathrm{Nil}(\mathbb{Z}/n\mathbb{Z}) = \langle p_1 \cdots p_r \rangle$

c) $\varphi : X \longrightarrow \mathbb{F}$ is nilpotent

$\Rightarrow \exists\, k \in \mathbb{N}$ such that $\varphi^k = 0$

$\Rightarrow \varphi^k(x) = \varphi(x)^k = 0 \quad \forall x \in X$

$\Rightarrow \varphi(x) = 0 \quad \forall x \in X \quad \Rightarrow \varphi = 0$

(14) a) $x \in R$ is nilpotent

$\Rightarrow \exists k \in \mathbb{N}$ such that $x \cdot x^k = 0$.

(Take the minimal one.)

$\Rightarrow$ If $k = 0$, then $x^k = 1$, hence $x = 0$.

If $k > 0$, then $x, x^k \neq 0$ (else k is not minimal), hence x is a zero divisor.

b) $x \in R$ is nilpotent, $rx = xr$

$\Rightarrow \exists k \in \mathbb{Z}^+$ such that $x^k = 0$.

$\Rightarrow \exists k \in \mathbb{Z}^+$ such that $(rx)^k = r^k x^k = 0$

$\Rightarrow rx$ is nilpotent

c) $x \in R$ is nilpotent

$\Rightarrow \exists k \in \mathbb{N}$ such that $x^{k+1} = 0$.

$\Rightarrow (1-x)(1+x+x^2+ \dots + x^k) = 1 - x^{k+1} = 1$

$\Rightarrow 1-x \in R^*$, analogously $1+x$.

d) $x \in R$ is nilpotent, $u \in R^*$

$\Rightarrow x/u$ is nilpotent $\Rightarrow 1 + x/u \in R^*$

$\Rightarrow u + x = u(1 + x/u) \in R^*$

(20) $(a_i), (b_i) \in R$, where $R = \bigoplus_{\mathbb{N}} \mathbb{Z}$

$\Rightarrow$ cofinitely many $a_i = b_i = 0$

$\Rightarrow$ cofinitely many $a_i + b_i = a_i b_i = 0$

$\Rightarrow (a_i + b_i), (a_i b_i) \in R$

$\Rightarrow R$ is a subring of $\prod_{\mathbb{N}} \mathbb{Z}$

However, $1 \in \prod_{\mathbb{N}} \mathbb{Z}$ is not in R

$\Rightarrow R$ is a ring without unit.

(21) a) We have a natural bijection

$$\begin{aligned}
\varphi : P(X) &\longrightarrow R = \{ f : X \to \mathbb{F}_2 \} \\
A &\longmapsto 1_A : X \to \mathbb{F}_2 \\
& \qquad x \longmapsto \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}
\end{aligned}$$

- $1_{A \Delta B}(x) = 0 \iff x \notin A \Delta B$

$\iff x \in A \equiv x \in B \iff 1_A(x) = 1_B(x)$

Hence $1_{A\Delta B}(x) = 1_A(x) + 1_B(x)$.

Hence $\varphi(A \Delta B) = 1_{A\Delta B} = 1_A + 1_B = \varphi(A) + \varphi(B)$.

- $1_{A\cap B}(x) = 1 \iff x \in A \cap B$

$\iff x \in A \wedge x \in B \iff 1_A(x) = 1_B(x) = 1$

Hence $1_{A \cap B}(x) = 1_A(x) \cdot 1_B(x)$.

Hence $\varphi(A \cap B) = 1_{A\cap B} = 1_A \cdot 1_B = \varphi(A) \cdot \varphi(B)$.

b) • $A \cap B = B \cap A \quad \forall A, B \subset X$ (commut.)

• $X \cap A = A \quad \forall A \subset X$ (identity)

• $A \cap A = A \quad \forall A \subset X$ (Boolean)

23 $D \in \mathbb{Z}$ square-free $\quad K = \mathbb{Q}(\sqrt{D})$

$\mathcal{O}_K = \{ \alpha \in K \mid \exists f \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0 \}$

$= \{ \alpha \in K \mid m_\alpha \in \mathbb{Z}[x] \}$

by Gauss' lemma

- $\alpha = a + b\sqrt{D}, \quad b \neq 0$

  $\Rightarrow \alpha^2 = (a^2 + b^2 D) + 2ab\sqrt{D}$

  $\Rightarrow m_\alpha = x^2 - 2ax + (a^2 - b^2 D)$

- $\alpha \in \mathcal{O} \Rightarrow 2a, \; a^2 - b^2 D \in \mathbb{Z}$

  - $D \equiv 1 \pmod 4 \Rightarrow a^2 - b^2 \in \mathbb{Z} \Rightarrow a - b \in \mathbb{Z}$

  - $D \equiv 2,3 \pmod 4 \Rightarrow a, b \in \mathbb{Z}$

$$\therefore \mathcal{O}_K = \mathbb{Z}[\omega], \quad \omega = \begin{cases} \dfrac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \\ \sqrt{D} & D \equiv 2,3 \pmod 4 \end{cases}$$

$f \in \mathbb{Z} \qquad \mathcal{O}_f = \{ a + b\omega \mid a \in \mathbb{Z}, \; b \in f\mathbb{Z} \}$

- $(a + b\omega) \cdot (c + d\omega)$

  $= (ac + bd\omega^2) + (ad + bc)\omega$

  $= (ac + bd(\omega^2 - \omega)) + (ad + bc + 1)\omega$

  $\in \mathcal{O}_f$, hence $\mathcal{O}_f \subset \mathcal{O}_K$ is a subring

- $\mathcal{O}_K / \mathcal{O}_f = \{ b\omega \mid b \in \mathbb{Z}/f\mathbb{Z} \} \simeq \mathbb{Z}/f\mathbb{Z}$

  Hence $[\mathcal{O}_K : \mathcal{O}_f] = f$.

$R \subset \mathcal{O}_K$ subring with 1

- $\mathcal{O}_K \simeq \mathbb{Z}^2$ as an Abelian group.
- $R = \mathbb{Z} + G\omega$ for some subgroup $G \subset \mathbb{Z}$.
- $[\mathcal{O}_K : R] = [\mathbb{Z} : G] = f$

$$\Rightarrow \quad G = f\mathbb{Z} \quad \Rightarrow \quad R = \mathcal{O}_f$$

§ 7.2

(3) $$R[\![x]\!] = \left\{ \sum_{n \in \mathbb{N}} a_n x^n \;\middle|\; a_n \in R \quad \forall n \in \mathbb{N} \right\}$$

- Define a norm on $R[\![x]\!]$:

$$\|f\| = \begin{cases} 2^{-n} & f \in \langle x^n \rangle,\ f \notin \langle x^{n+1} \rangle \\ 0 & f = 0 \end{cases}$$

$$d(f,g) = \|f - g\| \longrightarrow x\text{-adic topology}$$

- Define the polynomial approximations

$$f = \sum_{n \in \mathbb{N}} a_n x^n \longrightarrow f_n = \sum_{k < n} a_k x^k$$

Note that $f_n \longrightarrow f$ x-adically.

a) By construction,

$$f_n + g_n \longrightarrow f+g \qquad f_n g_n \longrightarrow fg$$

Therefore, by continuity, the ring axioms which are known to hold in $R[x]$, also hold in the x-adic completion $R[\![x]\!]$.

For example,

$$\begin{array}{ccccccc} f_n(g_n+h_n) & - & f_n g_n & - & f_n h_n & = & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ f(g+h) & - & fg & - & fh & = & 0 \end{array}$$

$$\therefore \quad f(g+h) = fg + fh$$

b) Consider the polynomial approximations

$$f_n = \sum_{k<n} x^k \longrightarrow f = \sum_{n \in \mathbb{N}} x^n$$

Multiplying times $1-x$, we have

$$(1-x)f = \lim (1-x) f_n = \lim (1-x^n) = 1$$

Therefore, $\frac{1}{1-x} = f$.

c) $f \in \langle x \rangle \Longrightarrow f^n \in \langle x^n \rangle$

$\Longrightarrow g_n = \sum_{k<n} f^k$ has eventually const. poly. approx. in every degree.

$\Longrightarrow g_n$ converges, $g = \sum_{n \in \mathbb{N}} f^n$ well def.

$\Longrightarrow (1-f)\, g = 1 \Longrightarrow 1-f \in R[\![x]\!]^*$

Similarly, $a+f \in R[\![x]\!]^* \ \forall a \in R^*$.

(12) G finite group, $R[G]$ group ring

$N = \sum G \Longrightarrow gN = N = Ng \quad \forall g \in G$

$\Longrightarrow N \in C_{R[G]}(1 \cdot G) = C_{R[G]}(R[G]) = Z(R[G])$.

Because coefficients (in R) commute with "variables" (in G).

§ 7.3

(25) The binomial coefficients are defined as follows:

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!\,(n-k)!} & k \in \{0, 1, \dots, n\} \\ 0 & \text{any other } k \in \mathbb{Z} \end{cases}$$

By induction on n, we shall show

$$(a+b)^n = \sum_{k\in\mathbb{Z}} \binom{n}{k} a^k b^{n-k}$$

The base case is trivial:

$$(a+b)^0 = \sum_{k\in\mathbb{Z}} \binom{0}{k} a^k b^{-k} = \binom{0}{0} a^0 b^0 = 1$$

The inductive case reduces to Pascal's theorem:

$$(a+b)^{n+1} = (a+b)\cdot \sum_{k\in\mathbb{Z}} \binom{n}{k} a^k b^{n-k}$$

$$= \sum_{k\in\mathbb{Z}} \binom{n}{k} \left(a^{k+1} b^{n-k} + a^k b^{n-k+1}\right)$$

$$= \sum_{k\in\mathbb{Z}} \left[\binom{n}{k} + \binom{n}{k+1}\right] a^{k+1} b^{n-k}$$

$$= \sum_{k\in\mathbb{Z}} \binom{n+1}{k+1} a^{k+1} b^{n-k}$$

29 $x, y \in \mathrm{Nil}(R) \Rightarrow \exists\, m, n \in \mathbb{N} : x^{m+1} = y^{n+1} = 0$

$$\Rightarrow (x+y)^{m+n+1} = \sum_{k\in\mathbb{Z}} \binom{m+n+1}{k+1} \underbrace{a^{k+1}}_{\substack{\text{Vanishes} \\ \text{for } k \geq m.}} \underbrace{b^{m+n-k}}_{\substack{\text{Vanishes} \\ \text{for } k < m.}} = 0$$

§ 7.4

(8) R integral domain, $a, b \in R$

$(a) = (b) \Rightarrow a = ub \wedge b = va$

$\Rightarrow a(1 - uv) = 0 \Rightarrow a = 0 \vee uv = 1$

- If $a = 0$, then $b = 0 = 1 \cdot a$.
- If $a \neq 0$, then $uv = 1$, hence $u \in R^*$.

Counterexample when R is not a domain:

- $R = \dfrac{\mathbb{C}[X,Y]}{\langle XY^2 \rangle} \longrightarrow$ Not prime!
- $x = x(1-y^2) \Rightarrow \langle x \rangle = \langle x(1+y) \rangle$
- Suppose $\exists u \in R^*$ s.t. $xu = x(1+y)$.

$\Rightarrow 1 + y - u \in \text{Ann}(x) = \langle y^2 \rangle$

$\Rightarrow 1 + y - u \in \mathbb{C}[y]$, because $xy^2 = 0$

$\Rightarrow \exists U \in \mathbb{C}[Y]$ representative

$\Rightarrow \langle XY^2, U \rangle \subset \langle X, U \rangle \subsetneq \mathbb{C}[X,Y]$

$\Rightarrow u \in \langle x, u \rangle \subsetneq R \Rightarrow u \notin R^*$

(9) $R = \{ f : [0,1] \to \mathbb{R} \text{ cts.} \}$

$I = \{ f \in R \mid f(1/3) = f(1/2) = 0 \}$

- I is an ideal (easy)
- I is not prime:

$$x - 1/3,\ x - 1/2 \notin I, \text{ but } (x - 1/3)(x - 1/2) \in I$$

(15) $E = \mathbb{F}_2[x]$ $\qquad I = \langle \underbrace{x^2 + x + 1}_{d} \rangle$

a) Define

$$\varphi : E \longrightarrow \mathbb{F}_2 + \mathbb{F}_2 x \quad \mathbb{F}_2\text{-linear}$$

$$p \longmapsto r, \text{ where } p = dq + r$$

By the first iso. thm.,

$$E/I = E/\ker\varphi \simeq \operatorname{im}\varphi = \mathbb{F}_2 + \mathbb{F}_2 x$$

$$E/I = \{ \bar{0}, \bar{1}, \bar{x}, \overline{x+1} \}$$

b) By construction, $E/I \simeq \mathbb{F}_2^2 \simeq V_4$.

(You have to construct the table.)

c) d irreducible in a PID

$\Rightarrow I$ nonzero prime ideal of a PID

$\Rightarrow I$ maximal ideal of E

$\Rightarrow E/I$ is a field, $E/I \simeq \mathbb{F}_4$

§ 7.5

(5) Every nonzero element of $F[\![x]\!]$ is of the form $x^n u$ for some $u \in F[\![x]\!]^*$. Thus, its inverse in $F((x)) = F[\![x]\!][x^{-1}]$ is $x^{-n}u^{-1}$, where $u^{-1} \in F[\![x]\!]$ already. Hence,

$$F((x)) = \Big\{ \sum_{k \geqslant n} a_k x^k \;\Big|\; a_k \in F,\ n \in \mathbb{Z} \Big\}$$

§ 7.6

(1) $e \in Z(R) \Rightarrow Re,\ R(1-e)$ two-sided ideals

$$e \text{ idempotent} \Rightarrow \begin{cases} 1-e \text{ idempotent as well} \\ e(1-e) = 0 \end{cases}$$

The R-module homomorphism

$$\varphi : R \longrightarrow Re, \quad \varphi(x) = xe$$

is actually a ring homomorphism as well:

- $\varphi(xy) = xye = xye^2 = xe \cdot ye = \varphi(x) \cdot \varphi(y)$
- $\varphi(1_R) = e = 1_{Re}$

Analogously, $\psi : R \longrightarrow R(1-e)$. Then

$$\varphi \times \psi : R \longrightarrow Re \times R(1-e)$$
$$x \longmapsto (xe, \; x(1-e))$$

is a ring isomorphism.

11 Define a norm on $\mathbb{Z}$:

$$\|x\| = \begin{cases} q^{-1} & x = qr, \; q = p^k, \; p \nmid r \\ 0 & x = 0 \end{cases}$$

$$d(x,y) = \|x-y\| \longrightarrow \text{p-adic topology}$$

Then (x_n) is a Cauchy sequence iff, $\forall q = p^m$, the residue $\tilde{x}_q = x_n \pmod q$ is eventually constant.

Equivalence of Cauchy sequences:

$$(x_n) \sim (y_n) \iff \tilde{x}_q = \tilde{y}_q \text{ eventually}, \ \forall q = p^m$$

The metric completion of $\mathbb{Z}$ is

$$\mathbb{Z}_p = \{ (x_n) \text{ Cauchy} \} / \sim$$

a) Each $\tilde{x}_q$ is a finite (integer) approx.

$$\tilde{x}_q = \sum_{k<m} b_k p^k, \qquad b_k \in \{0, 1, \dots, p-1\}$$

to the actual value of $\lim x_n \in \mathbb{Z}_p$.

Obs: b_k does not depend on m. That is,

$$\tilde{x}_{qp} = \tilde{x}_q + b_m p^m, \qquad b_m: \text{ only new datum}$$

Collecting the information from every finite integer approximation, we have

$$\mathbb{Z}_p \cong \left\{ \sum_{k \in \mathbb{N}} b_k p^k \right\} = \left\{ \begin{matrix} \text{infinite base } p \\ \text{numbers} \end{matrix} \right\}$$

The ring operations of $\mathbb{Z}_p$ follow the usual rules of base p arithmetic. (Exercise.)

b) The p-adic topology is Hausdorff.

$\Rightarrow$ Constant Cauchy sequences are equivalent iff equal.

$\Rightarrow$ The completion map $\varphi: \mathbb{Z} \to \mathbb{Z}_p$ is injective.

Moreover, given nonzero elements

$$x = \sum_{m \in \mathbb{N}} a_m p^m \qquad y = \sum_{n \in \mathbb{N}} b_n p^n$$

$\Rightarrow \exists\, m, n \in \mathbb{N}$ such that $a_m, b_n \neq 0$

(Take the minimal ones.)

$\Rightarrow c_{m+n} = a_m b_n \pmod p$ is the minimal nonzero coefficient of $xy = \sum_{k \in \mathbb{N}} c_k p^k$.

$\Rightarrow xy \neq 0$

$\Rightarrow \mathbb{Z}_p$ is an integral domain, since x, y were chosen arbitrarily.

c) $f \in \langle p \rangle \implies f^n \in \langle p^n \rangle$

$\implies g_n = \sum\limits_{k<n} f^k$ has eventually const.

integer approx. $\tilde{g}_q \quad \forall q = p^m$.

$\implies g_n$ converges, $g = \sum\limits_{n \in \mathbb{N}} f^n$ well def.

$\implies (1-f)\, g = 1 \implies 1-f \in \mathbb{Z}_p^*$

On the other hand, given $b \not\equiv 0 \pmod p$

$\Rightarrow \bar{b} \in (\mathbb{Z}/q\mathbb{Z})^*, \quad \forall q = p^n,$

$\Rightarrow \forall q = p^n : \exists c_n \in \mathbb{Z} : bc_n \equiv 1 \pmod q$

$\Rightarrow bc_{n+k} \equiv bc_n \pmod q \Rightarrow c_{n+k} \equiv c_n \pmod q$

$\Rightarrow (c_n)$ is a Cauchy sequence.

$\Rightarrow b \cdot \lim c_n = \lim bc_n = 1 \Rightarrow b \in \mathbb{Z}_p^*$

d) Every nonzero element of $\mathbb{Z}_p$ is of the

form $p^n u$ for some $n \in \mathbb{N}$, $u \in \mathbb{Z}_p^*$.

(Exercise: Complete the proof.)

§ 8.2

2 R principal ideal domain

$I = \langle a \rangle \cap \langle b \rangle$ common multiples

$a, b \neq 0 \Rightarrow ab \neq 0 \Rightarrow I \neq 0$

$\Rightarrow \exists d \neq 0$ such that $I = \langle d \rangle$

$\Rightarrow d$ is a least common multiple of a, b.