Introduction to Rings and Fields

Prof Krishna Hanumanthu

Organized Results

complied by

Sarthak[1]

March 2022

To the genius **Teach**[2]
without whom
I'd have learnt about half
of what I did...

To **Prof Amber**[3]
for advising me to
take this course.

[1]vijaysarthak23@gmail.com

[2]the TA of the course

[3]Head of Math Dept., Shiv Nadar University

Contents

Part I

Rings

Chapter 1

Main definitions

February 1, 2022

Definition 1.0.1 (Rings)**.** $(R, +, \cdot)$ is a ring iff the following hold:

(a) $(R, +)$ is an abelian group.

(b) $\cdot\colon R \times R \to R$ such that there exists a $1 \in R$ such that for all $a, b, c \in R$, we have

  (i) $a \cdot b = b \cdot a$,

  (ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, and

  (iii) $a \cdot 1 = a$.

(c) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

Remark 1.0.2. We'll denote the additive and multiplicative identities of a ring by 0 and 1.

Definition 1.0.3 (Subrings)**.** Let R be a ring. Then S is a subring of S iff $S \subseteq R$, and addition and multiplication of R can be inherited to S as operations on S (that is, S is closed under these) such that these inherited operations make S a ring, and the multiplicative identities of S and R are equal.

Remark 1.0.4. To show the necessity of demanding the equality of multiplicative identities, consider $4 \in \{0, 2, 4\} \subseteq \mathbb{Z}/\mathbb{Z}6$.

Proposition 1.0.5 (An equivalent condition for being a subring)**.** *Let R be a ring and $S \subseteq R$. Then S is a subring of $R \iff$ the following hold:*

(a) S is closed under addition and multiplication.

(b) $-1, 1 \in S$.

Corollary 1.0.6.

(a) A subring of a subring is a subring of the parent ring.
(b) Intersection of subrings is a subring.

Proposition 1.0.7 (Non-examples of rings)**.**

(a) The set of $n \times n$ matrices with (entries in a field) follows everything except commutativity of multiplication.
(b) The nontrivial subgroups of the additive group of $\mathbb{Z}$ obey everything except they don't have 1.
(c) $\mathbb{Z}$ with usual addition but with multiplication taken be the usual addition, obeys everything except distributivity.
(d) $\left\{a + \frac{b}{2} \in \mathbb{Q} : a, b \in \mathbb{Z}\right\}$ is not a ring under the usual operations.

Proposition 1.0.8 (Examples of rings)**.**

(a) The zero ring with obvious addition and multiplication.
(b) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}[i]$, $\mathbb{C}$ with usual operations.
(c) $\mathbb{Z}/\mathbb{Z}n$ with usual operations.
(d) The set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ with pointwise addition and multiplication. We can also take the set of all functions, and not just continuous.

Proposition 1.0.9 (Product rings)**.** *Let R, R' be rings. Then the operations $(a, a')+(b, b') := (a + b, a' + b')$ and $(a, a')(b, b') := (ab, a'b')$ make $R \times R'$ into a ring.*

Remark 1.0.10. Unless stated otherwise, take $R \times R'$ to be the product ring.

Lemma 1.0.11 (Reducing fractions to lowest forms)**.** *Let $r \in \mathbb{Q}$. Then there exist integers $a, b \in \mathbb{Z}$, with $b \neq 0$, unique up to signs, such that $r = a/b$ and $\gcd(a, b) = 1$.*

Lemma 1.0.12 (Factors of prime powers)**.** *Let p be a positive prime and $n \geq 0$. Let $a \geq 0$ such that a divides p^n. Then there exists $0 \leq m \leq n$ such that $a = p^m$.*

Proposition 1.0.13 (Some subrings of $\mathbb{Q}$)**.** *Let p be a positive integer and let*

$$R := \left\{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1 \text{ and } p \text{ does not divide } b\right\},$$
$$R' := \left\{\frac{a}{p^n} \in \mathbb{Q} : a \in \mathbb{Z} \text{ and } n \in \mathbb{N}\right\}.$$

Then R, R' are rings (under usual operations) $\iff$ p is prime.

Remark 1.0.14. *Prove that $\mathbb{Z}/\mathbb{Z}n$ is not a subring of $\mathbb{C}$ for $n \geq 2$.*

Proposition 1.0.15 (Characterizing zero ring)**.** *Let R be a ring. Then the following are equivalent:*

(a) R *is a singleton.*
(b) $R = \{0\}$.
(c) $1 = 0$.
(d) 0 *is invertible under multiplication.*

Definition 1.0.16 (Units)**.** The elements of a ring R that have multiplicative inverses are called units.

Proposition 1.0.17 (Examples of units)**.**

(a) ± 1 *are always units in any ring.*
(b) In a nonzero ring, 0 *is not invertible.*
(c) $\{\text{units of } \mathbb{Z}\} = \{\pm 1\}$.
(d) $\{\text{units of } \mathbb{Q}\} = \mathbb{Q} \setminus \{0\}$.
(e) $\{\text{units of } \mathbb{Z}[i]\} = \{\pm 1, \pm i\}$.

Proposition 1.0.18 (Units form a multiplicative group)**.** *The units of a ring form a multiplicative group.*

Proposition 1.0.19 (When do rings become fields?)**.** *Let R be a ring. Then R is a field (under the same addition and multiplication)* $\iff$ *R is a nonzero ring with each nonzero element being a unit.*

Chapter 2

Polynomial rings

February 2, 2022

Definition 2.0.1 (Polynomial rings)**.** Let R be a ring. Then we set

$$R[x] := \left\{ \sum_{i=0}^{n} a_i x^i : n \in \mathbb{N} \text{ and } a_1, \ldots, a_n \in R \right\},$$

where the sums are just formal expressions which should be identified with the ordered tuples.

We define an equivalence relation on this $R[x]$ by declaring two polynomials $\sum_{i=0}^{m} a_i x^i$ and $\sum_{i=0}^{n} b_i x^i$ equal if their $a_i = b_i$ whenever a_i or b_i is nonzero. (Hence, there is only one zero "polynomial", etc.) Abusing notation, we denote the set of equivalence classes by $R[x]$ and the equivalence classes by representative elements.

The usual operations on $R[x]$ are defined as follows. The addition is like vector addition of tuples. The multiplication is defined as follows. For monomials ax^m and bx^n, we define $(ax^m)(bx^n) := (ab)x^{m+n}$ for any $a, b \in R$ and for any $m, n \geq 0$. For general polynomials, demanding distributivity (that is, $p(q+r) = pq+pr$) determines their product.

Proposition 2.0.2 ($R[x]$ is a ring)**.** *The above operations make $R[x]$ a ring for any ring R. Also, R can be embedded inside $R[x]$.*

Remark 2.0.3. Unless stated otherwise, take $R[x]$ to be a ring under the above usual operations.

Lemma 2.0.4. *Let R be a ring. Then R is nonzero $\iff$ $R[x]$ is nonzero.*

Definition 2.0.5 (Degree and leading coefficients of nonzero polynomials)**.** The degree of a nonzero polynomial $p = \sum_{i=0}^{n} a_i x^i \in R[x]$ is the greatest $i \in \mathbb{N}$ such that $a_i \neq 0$. The corresponding coefficient is called the leading coefficient of p.

Remark 2.0.6. We leave the degree of the zero polynomial undefined.

Proposition 2.0.7 (Division in $R[x]$)**.** *Let R be a ring. Let $f, g \in R[x]$ such that $g \neq 0$ and the leading coefficient of g is a unit in R. Then there exist unique $q, r \in R[x]$ such that $f = qg + r$ and $r = 0$ or else, degree of r is less than that of g.*

Remark 2.0.8. If $p \in R[x]$, then we'll denote by $p(x)$ the obvious quantity, no longer viewing the previous "sums" as formal objects, but as actual sums (in R).

Proposition 2.0.9 (Sums and products of polynomials are pointwise)**.** *Let R be a ring, $a \in R$ and $f, g \in R[x]$. Then $(f + g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$.*

Corollary 2.0.10 (Factor theorem)**.** *Let R be a ring, $p \in R[x]$ and $\alpha \in R$. Then $x - \alpha$ divides p (that is, the remainder is zero) $\iff p(\alpha) = 0$.*

Proposition 2.0.11 (A generalized factor theorem for integral domains)**.** *Let R be a ring. Then the following are equivalent:*

(a) The product of nonzero elements is nonzero.

(b) For any $p \in R[x]$, any $n \geq 0$, and distinct $a_1, \ldots, a_n \in R$, if each $(x - a_i)$ divides p, then $\prod_{i=1}^{n}(x - \alpha_i)$ divides p.

Remark 2.0.12. The ring of polynomials in several variables can also be defines along the same lines. The important thing to identify is that for any $n \geq 1$, we have

$$R[x_1, \ldots, x_{n+1}] = R[x_1, \ldots, x_n][x_{n+1}].$$

Chapter 3

Ring homomorphisms

February 3, 2022

Definition 3.0.1 (Ring homomorphisms and isomorphisms)**.** Let R, R' be rings and $\phi\colon R \to R'$. Then ϕ is a ring homomorphism iff for every $a, b \in R$, we have

(a) $\phi(a+b) = \phi(a) + \phi(b)$,
(b) $\phi(ab) = \phi(a)\phi(b)$, and
(c) $\phi(1) = 1$.

A bijective ring homomorphism is called a ring isomorphism.

Remark 3.0.2. To show the necessity of (c), consider ϕ on a ring R given by $x \mapsto xe$ where e is idempotent and not equal to 1. ($3^2 \equiv 3 \mod 6$.) Also, the trivial group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ that maps everything to 0 is also ruled out by (c).

Corollary 3.0.3. *The inverse of a ring isomorphism is a ring homomorphism.*

Corollary 3.0.4. *Compositions of ring homomorphisms are ring homomorphisms.*

Proposition 3.0.5 (Restrictions of ring homomorphisms)**.** *Let $\phi\colon r \to R'$ be a ring homomorphism and S be a subring of R. Then $\phi[S]$ is a subring of R' and ϕ's restriction to S is again a ring homomorphism.*

Remark 3.0.6. Unless stated otherwise, take the sets in Proposition 1.0.8 to be rings under the usual operations.

Proposition 3.0.7 (Ring homomorphisms from $\mathbb{Z}$ to R)**.** *For any ring R, there exists a unique ring homomorphism from $\mathbb{Z}$ to R. It is given by*

$$n \mapsto \begin{cases} \sum_{i=1}^{n} 1, & n \geq 0 \\ -\sum_{i=1}^{-1} 1, & n < 0 \end{cases}.$$

Corollary 3.0.8 (The only ring homomorphism on $\mathbb{Z}$)**.** *The identity function is the only ring homomorphism on* $\mathbb{Z}$*.*

Proposition 3.0.9 (Ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/\mathbb{Z}n$)**.** *Let* $n \in \mathbb{Z}$*. Then* $n \mapsto \bar{n}$ *is a ring homomorphism from* $\mathbb{Z}$ *to* $\mathbb{Z}/\mathbb{Z}n$*.*

Proposition 3.0.10 (Substitution homomorphism)**.** *Let* R *be a ring and* $a \in R$*. Define* $\phi_a \colon R[x] \to R$ *as*

$$\phi_a(f) := f(a).$$

Then ϕ_a *is a ring homomorphism.*

Proposition 3.0.11 (Homomorphisms on product rings)**.**

(a) The projection functions on product rings are ring homomorphisms.

(b) Let R*,* S*,* S' *be rings and* $\psi \colon R \to S$*,* $\phi \colon S'$*. Define* $\xi \colon R \to S \times S'$ *as*

$$\xi(r) := (\phi(r), \psi(r)).$$

Then ξ *is a ring homomorphism* $\iff$ ϕ*,* ψ *are ring homomorphims.*

Definition 3.0.12 (Kernel of a ring homomorphism)**.** Let R, R' be rings and $\phi \colon R \to R'$ be a ring homomorphism. Then we define $\ker \phi := \{a \in R : \phi(a) = 0\}$.

Remark 3.0.13. Hence, a $\ker \phi$ is the kernel if ϕ is viewed as the group homomorphism from R to R' taken as additive groups.

Corollary 3.0.14 (Kernel of the substitution homomorphism)**.** *Let* R *be a ring and* $a \in R$*. Then* $\ker \phi_a = \{(x - a)f : f \in R[x]\}$*.*

Corollary 3.0.15. *The kernel of a ring homomorphism contains* $1 \iff$ *the codomain ring is the zero ring.*

Proposition 3.0.16. *The images of units under ring homomorphisms are units.*

Remark 3.0.17. The converse needn't be true: Take the inclusion map from $\mathbb{Z}$ into $\mathbb{Q}$.

Chapter 4

Ideals

February 4, 2022

Definition 4.0.1 (Ideals)**.** Let R be a ring and $I \subseteq R$. Then I is an ideal of R iff

(a) I is a subgroup of R taken as the additive group, and
(b) for any $a \in I$, we have that $ar \in I$ for all $r \in R$.

Corollary 4.0.2 (Immediate consequences)**.**

(a) Let I be an ideal of a ring R. Then the following are equivalent:
  (i) $I = R$.
  (ii) I is a subring of R.
  (iii) $1 \in I$.
(b) The only ideals of $\mathbb{Z}$ are $\mathbb{Z}n$ for $n \in \mathbb{Z}$.
(c) Kernels of ring homomorphisms are ideals.
(d) Let R be a ring and $p \in R[x]$. Then the set of all polynomials in $R[x]$ divisible by p forms an ideal.

Proposition 4.0.3 (Characterizing fields with their ideals)**.** *Let R be a nonzero ring. Then R is a field $\iff$ its only ideals are $\{0\}$ and R.*

Remark 4.0.4. Ideals of a subring might not be the ideals of a the parent ring: consider $\mathbb{Z}2$, an ideal of $\mathbb{Z}$ which is not an ideal of $\mathbb{R}$.

Proposition 4.0.5 (Ideals of $K[x]$)**.** *Let K be a field and I be a nonzero ideal of $K[x]$. Let α be the least degree of polynomials in $I \setminus \{0\}$ and $f \in I$ be of degree α. Then $I = (f)$.*

Corollary 4.0.6. *A ring homomorphism whose domain ring is a field and the codomain ring is nonzero, is injective.*

Definition 4.0.7 (Ideals generated by sets)**.** Let R be a ring and $S \subseteq R$. Then we denote by (S), the smallest ideal of R containing S.

Remark 4.0.8. We'll use the usual notation that Artin uses for denoting the product and sum of sets, and product and sum of a set with an element.

Corollary 4.0.9 (Characterizing ideals generated by a set)**.** *Let R be a ring $S \subseteq R$. Then*

$$(S) = \{x_1 s_1 + \cdots x_n s_n : n \geq 0, x_i \in R, s_i \in S\}.$$

Definition 4.0.10 (Product of ideals)**.** Let I, J be ideals of a ring R. Then we denote by $I \cdot J$, the set of all the finite sums of elements of IJ.

Proposition 4.0.11 (Constructing ideals)**.** *Let I, J be ideals of a ring R. Then $I \cap J$, $I + J$, $I \cdot J$ are ideals. Further, $I + J = (I \cup J)$ and $I \cdot J = (IJ) \subseteq I \cap J$.*

Remark 4.0.12. The containment can be proper. For instance, $(2) \cdot (4) = (8) \subsetneq (4) = (2) \cap (4)$ in the usual ring $\mathbb{Z}$.

Proposition 4.0.13 (Product set of ideals need not be an ideal)**.** *Consider $\mathbb{Z}[x]$. Then $(2, x)(3, x)$ is not an ideal since $2x, 3x \in (2, x)(3, x)$ but $x = 3x - 2x \notin (2, x)(3, x)$. Further, $(2, x) \cdot (3, x) = (6, x)$.*

Proposition 4.0.14 (Principal ideals)**.** *Let R be a ring and $a, b \in R$. Then*

(a) $(a) = aR$,
(b) $(a) \cdot (b) = (ab) = (a)(b)$, *and*
(c) $(a, b) = (a) + (b)$.

Proposition 4.0.15 (A non-principal ideal)**.** $(2, x)$ *is non-principal in* $\mathbb{Z}[x]$.

Proposition 4.0.16 (Ideals under ring homomorphisms)**.** *Let $\phi \colon R \to R'$ be a ring homomorphism. Let I, I' be ideals of R, R' respectively and $S \subseteq R$. Then*

(a) if ϕ is surjective, then
  (i) $\phi[I]$ is an ideal of R',
  (ii) $\phi[(S)] = (\phi[S])$; and,
(b) $\phi^{-1}[I']$ is an ideal of R.

Remark 4.0.17. If surjectivity not obeyed, then $\phi[I]$ need not be an ideal. Consider the inclusion map from $\mathbb{Z}$ into $\mathbb{Q}$.

Definition 4.0.18 (Idempotents)**.** Let R be a ring and $a \in R$. Then a is idempotent iff $a^2 = a$.

Definition 4.0.19 (Nilpotent elements)**.** Let R be a ring and $a \in R$. Then a is nilpotent iff there exists an $n \geq 1$ such that $a^n = 0$. The set of all the nilpotents in R is called the nilradical of R.

Remark 4.0.20. This definition is equivalent to the one with $n \geq 1$ replaced with $n \geq 0$.

Corollary 4.0.21.

(a) 0 *is always nilpotent.*
(b) 1 *is nilpotent* $\iff$ *the ring is the zero ring.*
(c) The images of nipotents under ring homomorphisms are nilpotents.
(d) Nilradical of $\mathbb{Z} = \{0\}$*.*
(e) Nilradical of $\mathbb{Z}/\mathbb{Z}4 = \{\bar{0}, \bar{2}\}$*.*

Remark 4.0.22. The converse of (c) need not be true: Consider $n \mapsto \bar{n}$ from $\mathbb{Z}$ to $\mathbb{Z}/\mathbb{Z}4$.

Proposition 4.0.23. *The nilradical of a ring is an ideal.*

Chapter 5

Quotient rings

February 8, 2022

Proposition 5.0.1 (Quotient rings)**.** *Let I be an ideal of a ring R and let R/I to be the quotient group. In addition to the addition of cosets in R/I, we can define a product $*$ on R/I so that*

$$(a+I)*(b+I) = ab + I$$

for all $a, b \in R$. These operations make R/I into a ring.

Further, we have a natural surjective ring homomorphism from R to R/I given by $r \mapsto a + I$ with kernel I.

Remark 5.0.2. The above product need not be equal to the product set. Consider $(0+\mathbb{Z}2)*(0+\mathbb{Z}2)$ in $\mathbb{Z}/\mathbb{Z}2$.

Remark 5.0.3. Unless states otherwise, we'll assume R/I to be the quotient ring with the above operations. Also, we might denote $a + I \in R/I$ as $\bar{a}$.

Proposition 5.0.4 ($\mathbb{R}[x]/(x^2+1)$ isomorphic to $\mathbb{C}$)**.** *The function $\mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ given by $f + (x^2+1) \mapsto f(i)$ is well-defined and is a ring isomorphism.*

Remark 5.0.5. Note that i is not in the domain of f. This is remedied by declaring that $f(i)$ stands for the value at i of f's embedding inside $\mathbb{C}[x]$.

Proposition 5.0.6. *Let R be a ring. Then $R \cong R/\{0\}$.*

Chapter 6

Correspondence and isomorphism theorems

February 12, 2022

Theorem 6.0.1 (Correspondence theorem)**.** *Let $\phi\colon R \to R'$ be a surjective ring homomorphism. Then there is a one-to-one correspondence*

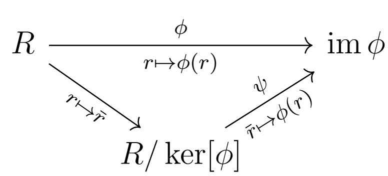
$$\{\textit{ideals of } R \textit{ containing } \ker\phi\} \leftrightarrow \{\textit{ideals of } R'\}$$

given as follows: $I \leftrightarrow I'$ iff $I' = \phi[I]$, or equivalently, iff $I = \phi^{-1}[I']$.

Theorem 6.0.2 (First isomorphism theorem)**.** *Let $\phi\colon R \to R'$ be a surjective ring homomorphism. Then there exists a unique function $\psi\colon R/\ker\phi \to R'$ such that*

$$\psi(r + I) = \phi(r).$$

Further, this ψ is an isomorphism with $\ker\psi = \ker\phi$.



Corollary 6.0.3 (Ideals of R/I)**.** *Let I be an ideal of a ring R. Then the ideals of R/I correspond to the ideals of R containing I.*

Proposition 6.0.4. *Let R be a ring and $\alpha \in R$. Then $R[x]/(x - \alpha) \cong R$.*

Proposition 6.0.5 ($\mathbb{R}[x]$ isomorphic to $\mathbb{C}$ and maximality of (x^2+1))**.** *The homomorphism* $\phi_i\colon \mathbb{R}[x] \to \mathbb{C}$ *is surjective with* $\ker \phi_i = (x^2+1)$. *Further, if* I *is an ideal in* $\mathbb{R}[x]$ *containing* (x^2+1)*, then* $I = (x^2+1)$ *or* $I = \mathbb{R}[x]$.

Proposition 6.0.6 (Ideals of $\mathbb{C}[t]/(t^2+1)$)**.** *The natural map* $\phi\colon \mathbb{C}[t] \to \mathbb{C}[t]/(t^2+1)$ *given by* $\phi(f) = f + (t^2+1)$ *is a surjective homomorphism with* $\ker \phi = (t^2+1)$. *We have that* $\mathbb{C}[t]/(t^2+1)$ *has four ideals given by* $\{0\}$, $(t \pm i) + (t^2+1)$ *and* $\mathbb{C}[t]/(t^2+1)$.

Proposition 6.0.7 (Extending homomorphisms over rings to over polynomial rings)**.** *Let* $\phi\colon R \to R'$ *be a ring homomorphism. Then* $\psi\colon R[x] \to R'[x]$ *defined as*

$$a_0 + \ldots + a_n x^n \mapsto \phi(a_0) + \cdots + \phi(a_n)x^n$$

is a ring homomorphism with

$$\ker \psi = (\ker \phi), \text{ and}$$
$$\operatorname{im} \psi = (\operatorname{im} \phi)[x],$$

where $(\ker \phi)$ *is the ideal generated by (the copy of)* $\ker \phi$ *in* $R[x]$.

Chapter 7

Prime and maximal ideals, and integral domains

February 13, 2022

Definition 7.0.1 (Integral domains)**.** Let ring R be a ring. Then R is called an integral domain iff R is not the zero ring, and for any $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

Definition 7.0.2 (Prime and maximal ideals)**.** Let I be a proper ideal of a ring R. Then I is called

(a) prime iff $ab \in I \implies a \in I$ or $b \in I$, and
(b) maximal iff for any ideal J, if $I \subsetneq J$, then $J = R$.

Corollary 7.0.3. *Any nonzero subring of an integral domain is an integral domain (with the inherited operations).*

Remark 7.0.4. The converse needn't be true. See Proposition 7.0.7.

Remark 7.0.5. For rings that are not integral domains, but contain integral domains, consider $\mathbb{Z}[x]/(x^2)$ and $\mathbb{Z} \times \mathbb{Z}$.

Proposition 7.0.6 (Characterizing prime and maximal ideals)**.** *Let I be an ideal of a ring R. Then*

(a) I is prime $\iff$ R/I is an integral domain, and
(b) I is maximal $\iff$ R/I is a field.

Thus, we also have that

(a) R is an integral domain $\iff$ $\{0\}$ is prime, and

(b) *R is a field $\iff$ $\{0\}$ is maximal.*

Proposition 7.0.7 (A non-integral domain containing an integral domain)**.** *$\mathbb{Z}[x]/(x^2)$ is a non-integral domain containing a copy of $\mathbb{Z}$.*

Proposition 7.0.8. *Maximal ideals are prime.*

Remark 7.0.9. Prime ideals need not be maximal. Consider the zero ideal in $\mathbb{Z}$. Even nonzero prime ideals need not be maximal. Consider any $(x-\alpha)$ in $R[x]$ for an integral domain R that is not a field.

Proposition 7.0.10 (Some prime ideals)**.**

(a) *The prime ideals of $\mathbb{Z}$ are exactly the zero ideal $\mathbb{Z}p$ for prime p's.*
(b) *If R is an integral domain, then the zero ideal and $(x-\alpha)$ for α's in R are prime.*

Remark 7.0.11. Not all zero ideals are prime. Consider $\mathbb{Z}/\mathbb{Z}4$.

Definition 7.0.12 (Unfactorizable polynomials)**.** Let R be a ring. Then $f \in R[x]$ is called factorizable iff there exist nonconstant polynomials $p, q \in R[x]$ such that $f = pq$. Otherwise, f is called unfactorizable.

Corollary 7.0.13 (Some maximal ideals)**.**

(a) *The maximal ideals of $\mathbb{Z}$ are exactly $\mathbb{Z}p$ for primes p's.*
(b) *For a field K, the maximal ideals of $K[x]$ are exactly of the form (f) for unfactorizable f's.*
(c) *The only maximal ideal of $\mathbb{R}/(x^2)$ is $(\bar{x})$.*
(d) *The only maximal ideal of $\mathbb{R}/(x^2+1)$ is the zero ideal.*
(e) *The maximal ideals of $\mathbb{C}/(x^2+1)$ are exactly $(\overline{x \pm i})$.*

Proposition 7.0.14 (Maximal ideals of $R[x, y]$ from $R[x]$)**.** *Let R be a ring and I be a maximal ideal of $R[x]$. Then $J + (y)$ is a maximal ideal of $R[x, y]$ where J is the ideal of $R[x, y]$ generated by I.*

Remark 7.0.15. This generalized to any coordinate in $R[x_1, \ldots, x_n]$ and even for infinite variables.

Proposition 7.0.16. *Let $p \in \mathbb{Z}$ be prime. Then (p, x) maximal in $\mathbb{Z}$.*
Also, it is the only proper ideal properly containing (p, x^2).

Proposition 7.0.17 (Existence of maximal ideals)**.** *Let I be a proper ideal of a ring R. Then there exists a maximal ideal in R containing I.*

Proposition 7.0.18. *Let R be a ring. Then R is an integral domain $\iff$ $R[x]$ is an integral domain.*

Proposition 7.0.19 (Prime and maximal ideals under ring homomorphisms)**.** *Let $\phi\colon R \to R'$ be a ring homomorphism and I, I' be ideals of R, R' respectively. Then the following hold:*

(a) if I, I' are prime, then
  (i) $\phi^{-1}[I']$ is prime, and
  (ii) ϕ is surjective and $\ker\phi \subseteq I \implies \phi[I]$ is prime;

(b) if I, I' are maximal and ϕ is surjective, then $\phi[I]$ and $\phi^{-1}[I']$ are maximal.

Remark 7.0.20. For (ii), consider the natural map $\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}4$, and I as the zero ideal. For (b), consider

(a) the embedding $\mathbb{Z} \to \mathbb{Q}$ and the inverse image of the zero ideal, and
(b) the embedding $\mathbb{Z} \to \mathbb{Z}[i]$ wherein (2) is maximal in $\mathbb{Z}$, but it's not in $\mathbb{Z}[i]$ since $(2i) \supsetneq (2)$.

Also, integral domain-ness need not be preserved even for surjective ring homomorphisms. Consider the naturam map $\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}4$.

Definition 7.0.21 (Adjoining elements to a ring)**.** Let S be a subring of R and $\alpha \in R$. Then we denote the smallest subring of R containing S and α by $S[\alpha]$.

Explicitly,

$$S[\alpha] = \{p(\alpha) : p \in S[x]\}.$$

Proposition 7.0.22 (Characterizing $R[\alpha]$)**.** *Let S be a subring of R and $\alpha \in R$. Then*

(a) $R[\alpha] \cong R[x]/\ker\phi_\alpha$, and
(b) $\ker\phi_\alpha = (x - \alpha) \cap R[x]$ which contains all the "polynomial relations" in $S[x]$ satisfied by α.

Proposition 7.0.23 (Existence of ring extensions)**.** *Let R be a ring and $p \in \mathbb{R}[x]$ be nonzero with degree $n \geq 1$. Then*

(a) R can be embedded consistently inside $R[x]/(p)$ via $\alpha \mapsto \bar{\alpha}$,
(b) $\bar{p}(\bar{x}) = \bar{0}$ (where $\bar{p} \in (R[x]/(p))[x]$ is the polynomial with the coefficients replaces with the images of the mentioned embedding),
(c) if p is monic (or the leading coefficient is a unit), then $R[x]/(p) \cong \{a_0 + \cdots + a_{n-1}^{n-1} : a_i \in R\}$.

Proposition 7.0.24. *Any prime ideal contains all the nilpotents in the ring.*

Proposition 7.0.25. *A nonzero ring that has all its proper ideals as prime, is a field.*

Proposition 7.0.26. *Finite integral domains are fields.*

Proposition 7.0.27 (Chinese remainder theorem)**.** *Let I, J be ideals of a ring R such that $I + J = R$. Then*

(a) $I \cap J = I \cdot J$,

(b) for any $a, b \in R$, there exists an $x \in R$ such that $x - a \in I$ and $x - b \in J$; or equivalently, the ring homomorphism $\phi\colon R \to R/I \times R/J$ defined by $a \mapsto (\bar{a}^I, \bar{a}^J)$ is surjective, and

(c) $R/I \cdot J \cong R/I \times R/J$.

Remark 7.0.28. *Do this!* This can be extended to more than two pairwise "co-prime" ideals.

7.1 Field of fractions

February 22, 2022

Proposition 7.1.1 (Field of fractions of an integral domain)**.** *Let R be an integral domain. Define the set of formal fractions*

$$\mathrm{Frac}(R) := \{a/b : a, b \in R, b \neq 0\}.$$

Then $a/b \equiv c/d$ iff $ad = cb$ is an equivalence relation on $\mathrm{Frac}(R)$. Abusing notation, denote the set of equivalence classes by $\mathrm{Frac}(R)$ again, and the equivalence classes by any of their representative elements.

We can define addition and multiplication on $\mathrm{Frac}(K)$ as

$$(a/b) + (c/d) := (ad + cb)/(bd),$$
$$(a/b)(c/d) := (ac)/(bd).$$

These operations turn $\mathrm{Frac}(R)$ into a field.

Further, $a \mapsto a/1$ embeds R into $\mathrm{Frac}(R)$.

Also, if R is an integral domain, then $R[x]$ is also an integral domain and we denote $\mathrm{Frac}\big(R[x]\big)$ by $R(x)$.

Proposition 7.1.2. *For any integral domain R, we have that $\mathrm{Frac}(R)$ is the smallest field containing a copy of R, i.e., any other such field contains a copy of $\mathrm{Frac}(R)$.*

Proposition 7.1.3. *A ring that is not an integral domain cannot be embedded inside a field.*

Definition 7.1.4 (Field extensions)**.** Let S be a subring of a field K so that S is an integral domain. Let $\alpha \in K$. Then we denote the smallest subfield of K containing S and α by $S(\alpha)$.

Explicitly,

$$S(\alpha) = \{p(\alpha)/q(\alpha) : p, q \in S(x) \text{ with } q(\alpha) \neq 0\}.$$

Proposition 7.1.5 (Some fields of fractions)**.**

(a) $\mathrm{Frac}(\mathbb{Z}) \cong \mathbb{Q}$*,*

(b) For any field K*, we have* $\mathrm{Frac}(K) \cong K$*,*

(c) For an integral domain R*, we have that*

$$\mathrm{Frac}(R)[x] \cong R(x).$$

(d) Let R *be a subring of a field* K *and* $\alpha \in K$*. Then*

$$\mathrm{Frac}(R)[\alpha] \cong R(\alpha).$$

7.2 Noetherian rings

February 22, 2022

Definition 7.2.1 (Finitely generated ideals)**.** An ideal I of a ring R is called *finitely generated* iff there exists a finite S such that $I = (S)$.

Definition 7.2.2 (Noetherian rings)**.** A ring R is called Noetherian iff all of its ideals are finitely generated.

Remark 7.2.3. Noetherian rings needn't be integral domains: Consider $\mathbb{Z}/\mathbb{Z}6$.

Definition 7.2.4 (Stabilization of ascending chain of ideals)**.** Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals of a ring R. Then it is said to stabilize iff there exists an $N \geq 1$ such that for all $n \geq N$, we have that $I_n = I_N$.

Proposition 7.2.5 (Characterization of Noetherian rings)**.** *Let* R *be a ring. Then* R *is Noetherian* $\iff$ *every ascending chain of ideals in* R *stabilizes.*

Remark 7.2.6. There can be non-stabilizing descending chains in Noetherian rings: Consider in $\mathbb{Z}$, the chain $(2) \supsetneq (4) \supsetneq (8) \supsetneq \cdots$.

Proposition 7.2.7 (Some Noetherian and non-Noetherian rings)**.**

(a) *K and $K[x]$ are Noetherian for any field K.*
(b) *$\mathbb{Z}$ is Noetherian.*
(c) *$R[x_1, x_2, \ldots]$ is non-Noetherian since $(x_1, x_2, \ldots)$ is not finitely generated.*
(d) *The set of all continuous functions $\mathbb{R} \to \mathbb{R}$ is non-Noetherian since the ascending sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$ where I_n contains all the functions which vanish for $x \geq n$, does not stabilize.*

Remark 7.2.8. Unlike integral domains, the subrings of Noetherian rings can be non-Noetherian: For an integral domain R, let $S := R[x_1, x_2, \ldots]$, which will be an integral domain and a non-Noetherian ring. But $\mathrm{Frac}(S) \supseteq S$ is Noetherian.

Proposition 7.2.9. *Quotient rings formed from Noetherian rings are Noetherian.*

Proposition 7.2.10. *Let R be a Noetherian ring and $S \subseteq R$. Then there exists a finite $T \subseteq S$ such that $(S) = (T)$.*

Theorem 7.2.11 (Hilbert's basis theorem)**.** *Let R be a ring. Then R is Noetherian $\iff$ $R[x]$ is Noetherian.*

Corollary 7.2.12. *Let R be a Noetherian ring and $n \geq 1$. Then $R[x_1, \ldots, x_n]$ is Noetherian too.*

Proposition 7.2.13. *Image of a Noetherian ring under a ring homomorphism is Noetherian.*

Proposition 7.2.14 (When can $R[\alpha]$ be Noetherian?)**.** *Let R be a Noetherian subring of a ring S and $\alpha \in S$. Then $R[\alpha]$ is Noetherian.*

Corollary 7.2.15. *$\mathbb{Z}[\sqrt{-5}]$ is Noetherian.*

Chapter 8

PID's and UFD's

March 4, 2022

Definition 8.0.1 (Divisors, associates, irreducibles, primes, gcd)**.** Let R be a ring and $a, b \in R$. Then we say that

(a) a is a divisor b or b is a multiple of a, written $a \mid b$ iff $b = ax$ for some $x \in R$,
(b) a is a proper divisor of b iff a is not a unit and there exists a non-unit element y such that $b = ay$,
(c) a and b are called associates iff $b = au$ for some unit u,
(d) a is called irreducible iff a is not a unit and a has no proper divisors,
(e) a is called prime iff $a \neq 0$, and a is not a unit such that for any $c, d \in R$, if $a \mid cd$, then $a \mid c$ or $a \mid d$, and
(f) an element $d \in R$ is a gcd for a, b iff g is a common divisor, and if every common divisor of a, b divides g.

Proposition 8.0.2 (Examples)**.**

(a) Let K be a field and $a, b \in K$. If one of these is nonzero, then the permissible gcd*'s are precisely $K \setminus \{0\}$. If both are zero, then entire K is permissible.*
(b) 2, 3, $1 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.
(c) Let R be an integral domain and $\alpha \in R$. Then $(x - \alpha)$ is irreducible in $R[x]$.
(d) In $\mathbb{Z}/\mathbb{Z}4$, the only prime is $\bar{2}$. In $\mathbb{Z}/\mathbb{Z}6$, the primes are exactly $\bar{2}$, $\bar{3}$ and $\bar{4}$.

Proposition 8.0.3 (Some properties in a general ring)**.** *Let R be a ring. Then*

(a) being an associate is an equivalence relation,
(b) associates preserve divisibility,
(c) all units are each other's associates,
(d) units have no proper divisors,

(e) *if p is nonzero and non-unit, then $p \in R$ is prime $\iff$ (p) is a prime ideal,*
(f) *if a is irreducible, then*
  (i) *(a) is a maximal principal ideal,*
  (ii) *a's divisors are precisely its associates and units;*
(g) *generalized idempotents that are not units are reducible,*
(h) *0 is reducible, and*
(i) *for $a, b, d \in R$, if $(a) + (b) = (d)$, then d is a* gcd *of a and b.*

Proposition 8.0.4 (Some properties in an integral domain)**.** *Let R be an integral domain. Then*

(a) *no associate of a nonzero element divides any of its associates properly,*
(b) *two elements are associates $\iff$ they divide each other,*
(c) *for a non-unit $a \in R$, the following are equivalent:*
  (i) *a is irreducible,*
  (ii) *(a) is a maximal principal ideal,*
  (iii) *a's divisors are precisely its associates and units;*
(d) *primes are irreducible.*

Remark 8.0.5. To show the necessity of integral domain-ness:

(a) For (a), consider $\bar{3} \in \mathbb{Z}/\mathbb{Z}6$ which properly divides itself since $\bar{3} = \bar{3} \cdot \bar{3}$.
(b) For (b), consider Proposition 8.0.7.
(c) For (c), consider $\mathbb{Z}/\mathbb{Z}6$ again.
(d) For (d) consider $\mathbb{Z}/\mathbb{Z}6$ in which $\bar{3}$ is prime and yet not irreducible.
  The converse needn't be true even in an integral domain: Consider $\mathbb{Z}[\sqrt{-5}]$ in which 2 is irreducible and yet not prime (2 doesn't divide $1 \pm \sqrt{-5}$, but divides their product 6).

Proposition 8.0.6. *In $\mathbb{Z}$, irreducibles and primes are the same, viz. the usual primes.*

Proposition 8.0.7 (Non-associates that divide each other)**.** *Consider the ring $R := C[0, 3]$ and $f, g \in R$ given by*

$$f(x) := \begin{cases} 1 - x, & x \in [0, 1] \\ 0, & x \in (1, 2] \\ x - 2, & x \in (2, 3] \end{cases} \quad \text{and} \quad g(x) := \begin{cases} f(x), & x \in [0, 2] \\ 2 - x, & x \in (2, 3] \end{cases}.$$

Then f and g are not associates, for any associates of R have no zeroes. However,

$f = gh$ *and* $g = fh$ *for*

$$h(x) := \begin{cases} 1, & x \in [0,1] \\ 3-2x, & x \in (1,2) \\ -1, & x \in [2,3] \end{cases} .$$

Proposition 8.0.8 (When can a gcd fail to exist?)**.** *Let R be an integral domain, a, b, x be irreducibles in R such that b is not an associate of a or x. Let $y \in R$ such that $ax = by$, say α. Then α and ab have no* gcd*.*

Corollary 8.0.9. 6 *and* $2 + 2\sqrt{-5}$ *have no* gcd *in* $\mathbb{Z}[\sqrt{-5}]$*.*

8.1 Principal ideal domains

March 5, 2022

Definition 8.1.1 (PID's)**.** An integral domain in which every ideal is principal is a called a principal ideal domain.

Remark 8.1.2. Rings with only prime ideals needn't be integral-domains: Consider $\mathbb{Z}/\mathbb{Z}4$.

Proposition 8.1.3 (Examples and non-examples of PID's)**.** *Some PID's:*

(a) $\mathbb{Z}$*.*
(b) K *and* $K[x]$ *for any field* K*.*

Some non-PID's:

(a) $R[x, y]$ *for any nonzero ring* R*.*
(b) $\mathbb{Z}[x]$*.*

Corollary 8.1.4. *PID's are Noetherian.*

Proposition 8.1.5 (Division algorithms in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$)**.** *Let $\alpha, \beta \in \mathbb{Z}[i]$ such that $|\beta|^2 \geq |\alpha|^2 > 0$. Then there exist $\eta, \xi \in \mathbb{Z}[i]$ such that $\beta = \alpha\eta + \xi$ and $0 \leq |\xi|^2 \leq |\alpha|^2/2$.*

The same holds for $\mathbb{Z}[i]$ replaced with $\mathbb{Z}[\sqrt{-2}]$ and wit $|\alpha|^2/2$ replaced with $3|\alpha|^2/4$.

Proposition 8.1.6. $\mathbb{Z}[i]$ *and* $\mathbb{Z}[\sqrt{-2}]$ *are PID's.*

Proposition 8.1.7 (gcd's in PID's)**.** *Let R be a PID and $a, b, d \in R$. Then d is a* gcd *of a and b $\iff$ $(a) + (b) = (d)$.*

Proposition 8.1.8. *In a PID, irreducibles are primes so that primality $\iff$ irreducibility.*

Proposition 8.1.9. *In a PID, nonzero prime ideals are maximal.*

Corollary 8.1.10. *For an integral domain R that is not a field, $R[x]$ is not a PID. (See Remark 7.0.9.)*

Remark 8.1.11. Subrings or super-rings of PID's needn't be PID's: Consider $R[x] \subseteq R(x)$ for any integral domain R that is not a field, or $\mathbb{Z} \subseteq \mathbb{Z}[x]$.

These also show that the images of PID's under ring homomorphisms needn't be PID's. (Take the inclusion homomorphism.)

Corollary 8.1.12. *Let R be a PID that's not a field and $a \in R$. Then (a) is maximal $\implies$ a is irreducible.*

Corollary 8.1.13 (Quotients of PID's)**.** *Let I be an ideal of a PID R. Then the ideals of R/I are principal.*

However, the R/I is an integral domain $\iff$ I is prime.

8.2 Unique factorization domains

March 5, 2022

Definition 8.2.1 (Non-terminating factorization)**.** Let R be a ring and $a \in R$. Then a is said to have a non-terminating factorization iff there exist $b_1, b_2, \ldots \in R$ such that each b_1 properly divides a, and each b_{i+1} properly divides b_i for $i \geq 1$.

Definition 8.2.2 (Irreducible factorization)**.** A factorization of a ring element into irreducibles is called an irreducible factorization of it.

Corollary 8.2.3 (Examples of non-terminating factorizations)**.**

(a) Nilpotents and idempotents have non-terminating factorizations in any ring.
(b) $2 = (\sqrt{2})^2 = (\sqrt[4]{2})^4 = (\sqrt[8]{2})^8 = \cdots$ has a non-teminating factorization in the integral domain $\mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$.

Proposition 8.2.4. *Let R be a ring and $a \in R$. If a has no non-terminating factorization, then a admits an irreducible factorization.*

Remark 8.2.5. The converse needn't be true. See Proposition 8.2.6.

Proposition 8.2.6 (Irreducible factorization $\not\Longrightarrow$ each factorization terminates)**.** *Let $S \subseteq \mathbb{Q}[x]$ be the set of polynomials whose constant and linear coefficients are integers. Then S is a ring with units ± 1. ($\mathbb{Q}[x]$ has more units.) Also, x is irreducible in S (and not in $\mathbb{Q}[x]$). Thus $x^2 \in S$ has an irreducible factorization in S given by*

$$x^2 = x \cdot x$$

despite also admitting a non-terminating factorization

$$x^2 = 2 \cdot \frac{x^2}{2} = 2^2 \cdot \frac{x^2}{2^2} = \cdots .$$

Proposition 8.2.7. *Let R be a ring and $x, y \in R$. Then $(x) \subsetneq (y) \neq R \implies y$ is a proper divisor of x.*

Further, if R is an integral domain and $x \neq 0$, then the converse holds as well.

Remark 8.2.8. For the necessity of integral domian-ness in the converse, consider $\bar{3} \in \mathbb{Z}/\mathbb{Z}6$ which is its own proper divisor.

Proposition 8.2.9 (When does an element have no non-terminating factorization?)**.** *Let R be an integral domain and $a \in R$ be nonzero. Then the following are equivalent:*

(a) a has no non-terminating factorization.
(b) For any $b_1, b_2, \ldots \in R$, the ascending chain of ideals $(a) \subseteq (b_1) \subseteq (b_2) \subseteq \cdots$ stabilizes.

Remark 8.2.10. Again $\mathbb{Z}/\mathbb{Z}6$ demonstrates the necessity of integral domain-ness.

The necessity of nonzero-ness of a is demonstrated by the fact that in a finite integral domain, 0 still has a non-terminating factorization.

Corollary 8.2.11. *In a Noetherian integral domain, no element has a non-terminating factorization.*

Definition 8.2.12 (Unique factorization)**.** Let R be a ring and $a \in R$. Then a is said to have a unique factorization iff

(a) a has an irreducible factorization, and
(b) if $p_1, \ldots, p_i, q_1, \ldots, q_j \in R$ are irreducibles such that $a = p_1 \cdot \cdots \cdot p_i = q_1 \cdot \cdots \cdot q_j$, then $i = j$ and, after possibly a rearrangement, p_k and q_k are associates for each k.

Definition 8.2.13 (UFD's)**.** An integral domain is called a unique factorization domain iff each non-zero and non-unit element admits a unique factorization.

Remark 8.2.14. A Noetherian integral domain might not be a UFD: Consider $\mathbb{Z}[\sqrt{-5}]$ in which $2 \cdot 3 = (1+\sqrt{5})(1-\sqrt{-5})$, failing uniqueness.

Prove this rigorously! The ring of algebraic numbers[1] has no irreducibles (due to existence of n-th roots) and has 2 as a non-unit. Hence, 2 has no irreducible factorization here.

Proposition 8.2.15 (Characterizing UFD's)**.** *Let R be ring. Then R is a UFD $\implies$ irreducibles are prime.*

The converse holds if R is an integral domain in which each nonzero non-unit has an irreducible factorization.

Corollary 8.2.16. *A PID is a UFD.*

Remark 8.2.17. Converse needn't be true: $\mathbb{Z}[x]$ is a UFD (shown in Subsection 8.2.1) that is not a PID.

Corollary 8.2.18 (Examples of UFD's)**.**

(a) K and $K[x]$ for any field K.
(b) $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$.
(c) $R[x]$ for any UFD R. (See Subsection 8.2.1.)

8.2.1 When is $R[x]$ a UFD?

March 7, 2022

Remark 8.2.19. We'll consider only nonzero rings for this subsection.

Definition 8.2.20 (Prime products)**.** Let R be a ring. Then $a \in R$ is called a prime product iff there exists a natural $n \geq 0$, primes $p_1, \ldots, p_n$ and a unit u such that $a = up_1 \ldots p_n$.

Proposition 8.2.21 (Special prime factorization of pairs of prime products in integral domains)**.** *Let R be an integral domain and a, b be prime products. Then there exist $m, n \geq 0$, primes $p_1, \ldots, p_m, q_1, \ldots, q_n$, naturals $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \geq 1$, a natural $0 \leq r \leq m, n$, and units u, v such that*

(a) $a = up_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $b = vq_1^{\beta_1} \cdots q_n^{\beta_n}$,
(b) $i \neq j \implies$ neither of the pairs p_i, p_j and q_i q_j are associates,
(c) $i \leq r \implies p_i$, q_i are associates, and
(d) $i, j > r \implies p_i$, q_j are not associates.

[1]This is the ring containing all the complex numbers satisfying monic polynomials in $\mathbb{Z}[x]$.

Proposition 8.2.22 (Divisors of prime products in integral domains)**.** *Let R be an integral domain, $n \geq 0$ be natural, $p_1, \ldots, p_n$ be primes, $\alpha_1, \ldots, \alpha_n \geq 0$ be naturals and u be a unit. Then the divisors of $up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ are precisely*

$$\left\{vp_1^{\beta_1} \cdots p_n^{\beta_n} : \text{ } v \text{ is a unit and } 0 \leq \beta_i \leq \alpha_i\right\}.$$

Proposition 8.2.23 (gcd's of prime products in integral domains)**.** *Let R be an integral domain, $m, n \geq 0$ be natural, $p_1, \ldots, p_m, q_1, \ldots, q_m$ be primes, $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \geq 0$ be naturals, u, v be units and $0 \leq r \leq m, n$ be a natural such that*

(a) $i \neq j \implies$ neither of the pairs p_i, p_j and q_i, q_j are associates,
(b) $i \leq r \implies p_i$, q_i are associates, and
(c) $i, j > r \implies p_i$, q_j are not associates.

Let $\delta_i := \min\{\alpha_i, \beta_i\}$ for $i \leq r$. Then

$$p_1^{\delta_1} \cdots p_r^{\delta_r}$$

is a gcd *of $up_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $vq_1^{\beta_1} \cdots q_n^{\beta_n}$.*

Definition 8.2.24 (gcd's of finite nonempty sets)**.** Let R be a ring and S be a finite nonempty set, say $S = \{a_1, \ldots, a_n\}$ for $n \geq 1$. Then d is called a gcd of S iff

(a) d divides each a_i, and
(b) e divides each $a_i \implies e \mid d$.

Corollary 8.2.25. *Let S be a nonempty set of prime products and $d \in R$. Then d is a* gcd *of $S \cup \{0\} \iff d$ is a* gcd *of S.*

Corollary 8.2.26. *A subset S of a ring has 0 as a* gcd $\iff S = \{0\}$.

Proposition 8.2.27. *Any nonempty set of prime products in an integral domain has a* gcd *that is itself a prime product.*

Lemma 8.2.28. *Irreducibles in a integral domain R are irreducible in $R[x]$ as well.*

Corollary 8.2.29. *In a UFD, any nonempty finite set has a* gcd*.*

Lemma 8.2.30 (Quotients in integral domains)**.** *Let R be an integral domain and $a, b \in R$ with b nonzero such that $b \mid a$. Then there exists a unique $x \in R$, denoted by a/b, such that $a = bx$.*

Lemma 8.2.31. *Let R be an integral domain d be a* gcd *of a finite nonempty subset S. Then 1 is a* gcd *of $\{a/d : a \in S\}$.*

Lemma 8.2.32. *Let R be a ring, $f \in R[x] \setminus \{0\}$ and $\alpha \in R$. Then $\alpha \mid f$ in $R[x]$ $\iff$ α divides all the coefficients of f in R.*

Definition 8.2.33 (Primitive polynomials)**.** Let R be a ring and $p \in R[x]$. Then p is called primitive iff

(a) $p \neq 0$ and $\deg p > 0$, and
(b) 1 is a gcd of p's coefficients.

Lemma 8.2.34. *For any ring, the proper divisors of a primitive polynomial are primitive polynomials.*

Lemma 8.2.35. *Let R be an integral domain and $f \in R[x]$ be primitive. Then f has no non-terminating factorization in $R[x]$ and hence has an irreducible factorization in $R[x]$.*

Definition 8.2.36 (Factorization domains)**.** An integral domain R is called a factorization domain iff every nonzero non-unit admits an irreducible factorization.

Proposition 8.2.37. *Let R be an FD and $f \in R[x]$ be a nonzero non-unit polynomial. Then there exists an irreducible factorization of f in $R[x]$.*

Proposition 8.2.38. *Let R be a UFD and $f \in R[x]$ be irreducible. Then $f \neq 0$ and*

(a) $\deg f = 0 \implies$ *the corresponding constant $c \in R$ is prime, and*
(b) $\deg f > 0 \implies$ *f is primitive.*

Lemma 8.2.39. *Let R be an integral domain, S be a nonempty finite subset and $b \in R$. Let d be a* gcd *of S and D be a* gcd *of $\{ab : a \in S\}$. Then D, bd are associates in R.*

Lemma 8.2.40. *Let R be a UFD, $f, g \in R[x]$ be primitive and $c, d \in R$ such that $cf(x) = dg(x)$. Then c, d are associates in R.*

Lemma 8.2.41. *Let R be a ring and $p \in R$ be prime. Then $\big(R/(p)\big)[x]$ is an integral domain.*

Define $\phi_p \colon R[x] \to \big(R/(p)\big)[x]$ as

$$a_0 + \cdots + a_n x^n \mapsto \overline{a_0} + \cdots + \overline{a_n} x^n$$

where $a \mapsto \bar{a}$ is the natural map from R to $R/(p)$. Then ϕ_p is a ring homomorphism.

Lemma 8.2.42 (Gauss' lemma)**.** *For an integral domain, the product of primitive polynomials is a primitive polynomial.*

Proposition 8.2.43. *For a UFD R, primes in R are prime in $R[x]$ as well.*

Lemma 8.2.44. *Let R be a UFD and $f \in \operatorname{Frac}(R)[x] \setminus \{0\}$ such that $\deg f > 0$. Then*

(a) there exist $c \in K \setminus \{0\}$ and a primitive $f_0 \in R[x]$ such that $f(x) = cf_0(x)$,
(b) these c's and f_0's are unique up to association in R, and
(c) $f \in R[x] \iff$ one (and hence all) of such c's are in R.

Lemma 8.2.45. *For any ring, nonconstant irreducible polynomials are primitive.*

Proposition 8.2.46. *Let R be an integral domain and $f \in R[x]$ be nonconstant and irreducible. Then f is irreducible in $\operatorname{Frac}(R)[x]$.*

Proposition 8.2.47. *Let R be a UFD and $f, g \in R[x]$ such that f is primitive and $f \mid g$ in $\operatorname{Frac}(R)[x]$. Then $f \mid g$ in $R[x]$.*

Theorem 8.2.48. *If R is a UFD, then $R[x]$ is a UFD.*

Corollary 8.2.49. *Let R be a UFD and $n \geq 1$. Then $R[x_1, \ldots, x_n]$ is a UFD.*

Proposition 8.2.50. *Let R be a UFD. Then $R[x_1, x_2, \ldots]$ is also a UFD.*

8.3 Eisenstein's criterion

March 10, 2022

Lemma 8.3.1 (Factors of monomials in integral domains)**.** *Let R be an integral domain, $\alpha \in R \setminus \{0\}$ and $k \geq 0$. Then any divisor of αx^k in $R[x]$ is of the form bx^i for $b \in R \setminus \{0\}$ $0 \leq i \leq k$.*

Proposition 8.3.2 (Eisenstein's criterion)**.**

(a) Let R be an integral domain, $f \in R[x]$ be nonzero and $p \in R$ be a prime such that

  (i) p does not divide the leading coefficient,
  (ii) p divides all the remaining coefficients, and
  (iii) p^2 doesn'does not divide the constant term.

  Then f is irreducible in $\operatorname{Frac}(R)[x]$.

(b) Let R be a UFD and $f \in R[x]$ be primitive, and irreducible in $\operatorname{Frac}(R)[x]$. Then f is irreducible in $R[x]$ as well.

Proposition 8.3.3 (Irreducibility of $f(g(x))$)**.** *Let R be an integral domain and $f, g \in R[x]$ with f irreducible and g having an inverse in $R[x]$, as functions from R to R. Let $h \in R[x]$ be such that as functions from R to R, we have*

$$h(x) = (f \circ g)(x).$$

Then h too is irreducible in $R[x]$.

Lemma 8.3.4. *Let R be an integral domain and $a, p, \alpha \in R$ with p prime such that $p \nmid a$ and $a \mid \alpha p$. Then $a \mid \alpha$.*

Proposition 8.3.5 (Applications of Eisenstein's criterion)**.** *For $\mathbb{Z}$, the following are irreducible in both in $\mathbb{Z}[x]$, as well as in $\mathbb{Q}[x]$:*

(a) $f(x) := x^3 + 3x^2 + 2$.
(b) $g(x) := x^{p-1} + x^{p-2} + \cdots + 1$ *for any positive prime in $\mathbb{Z}$.*

Chapter 9

Miscellaneous topics in ring theory

9.1 Characteristics of ring

March 11, 2022

Definition 9.1.1 (Characteristic)**.** Let R be a ring and ϕ be the unique ring homomorphism from $\mathbb{Z}$ to R. Then the non-negative integer n for which $\ker \phi = \mathbb{Z}n$, is called the characteristic of R, denoted by $\operatorname{char}(R)$.

Proposition 9.1.2. *Let $n \geq 0$. Then $\operatorname{char}(\mathbb{Z}/\mathbb{Z}n) = n$.*

Proposition 9.1.3. *Let R and S be rings such that there exists an injective ring homomorphism $\phi\colon R \to S$. Then $\operatorname{char}(R) = \operatorname{char}(S)$.*

Corollary 9.1.4. *The characteristic of a subring is the same as that of the parent ring.*

Lemma 9.1.5. *Let I be an ideal of a ring R and ϕ_R and $\phi_{R/I}$ be the respective ring homomorphisms from $\mathbb{Z}$ to R and R/I. Then*

$$\ker \phi_{R/I} = \phi_R^{-1}[I].$$

Proposition 9.1.6. *Characteristic of an integral domain is either 0 or a positive prime integer.*

Remark 9.1.7. Converse needn't be true:

(a) For $R := \mathbb{Z}[x, y]$ and $I := (xy)$, we have that R/I is not an integral domain and yet $\operatorname{char}(R/I) = 0$.

(b) For $R := (\mathbb{Z}/\mathbb{Z}p)[x]$ and $I := (x^2)$ for a prime integer p, we have that R/I is not an integral domain and still $\text{char}(R/I) = p$.

Proposition 9.1.8 (Characterizing characteristics)**.** *Let R be a ring with* $\text{char}(R) > 0$*. Then* $\text{char}(R)$ *is the minimum number of times that 1_R must be added to get 0_R.*

Proposition 9.1.9. *Let R be a ring and ϕ be the ring homomorphism from $\mathbb{Z}$ to R such that $\phi(n)$ is a unit for each $n \neq 0$. Then R contains a copy of rationals.*

9.2 Endomorphisms on $\mathbb{Z}/\mathbb{Z}n$

March 11, 2022

Definition 9.2.1 (Endomorphisms)**.** Let G be a group. Then an endomorphism on G is a group homomorphism from G to itself.

Proposition 9.2.2 (Characterizing endomorphisms on $\mathbb{Z}/\mathbb{Z}n$)**.** *Let $n \in \mathbb{Z}$ and R be the set of all the endomorphisms on the additive group $\mathbb{Z}/\mathbb{Z}n$. Then we can define addition and multiplication on R as*

$$(\phi + \psi)(x) := \phi(x) + \psi(x),$$
$$\phi\psi := \phi \circ \psi.$$

These make R into a ring which is isomorphic to the ring $\mathbb{Z}/\mathbb{Z}n$ with an isomorphism $\Phi \colon \mathbb{Z}/\mathbb{Z}n \to R$ given by

$$\Phi_{\bar{a}}(\bar{x}) := \bar{a}\bar{x}$$

where $\alpha \to \bar{\alpha}$ is the natural map from $\mathbb{Z}$ to $\mathbb{Z}/\mathbb{Z}n$ and the product on the LHS is the product in $\mathbb{Z}/\mathbb{Z}n$.

9.3 Localization

March 11, 2022

Definition 9.3.1 (Multiplicative sets)**.** Let R be a ring. Then $S \subseteq R$ is called multiplicative iff $1 \in S$ and it is closed under multiplication.

Corollary 9.3.2 (Characterizing integral domains)**.** *Let R be a ring. Then R is an integral domain $\iff$ $R \setminus \{0\}$ is multiplicative.*

Proposition 9.3.3 (Characterizing primes)**.** *Let R be a ring and $p \in R$. Then p is prime $\implies$ $\{a \in R : p \nmid a\}$ is multiplicative.*

Further, the converse holds if $p \neq 0$.

Proposition 9.3.4 (Localization)**.** *Let R be a an integral domain and $S \subseteq R$ be multiplicative such that $0 \notin S$. Define*

$$S^{-1}R := \{a/s : a \in R, s \in S\}.$$

Then $a/s \equiv b/t$ iff $at = bs$ is an equivalence relation on $S^{-1}R$. We can define addition and multiplication on $S^{-1}R$ as

$$(a/s) + (b/t) := (at + bs)/(st),$$
$$(a/s)(b/t) := (ab)/(st).$$

These make $S^{-1}R$ into a ring.

The map $a \mapsto a/1$ embeds R into $S^{-1}R$, and for and $s \in S$, we have that $s/1$ is a unit in $S^{-1}R$.

Corollary 9.3.5. *Localization of an integral domain by a multiplicative set not containing 0 is an integral domain.*

Definition 9.3.6 (Local rings)**.** A ring R is called local iff it has only one maximal ideal.

Lemma 9.3.7. *Let I be a proper ideal of a ring R such that if $a \notin I$, then a is a unit. Then I is the only maximal ideal of R.*

Proposition 9.3.8 (Local rings from prime elements)**.** *Let R be an integral domain with $p \in R$ being prime and let*

$$S := \{a \in R : p \nmid a\}.$$

Then $S^{-1}R$ is local with $(p/1)$ being the only maximal ideal. Also,

$$(p/1) \supsetneq (p^2/1) \supsetneq \cdots$$

is a decreasing chain of ideals.

Part II

Fields

Chapter 10

Main definitions

March 17, 2022

Definition 10.0.1 (Fields)**.** $(F, +, \cdot)$ is a field iff the following hold:

(a) $(F, +)$ is an abelian group.
(b) $\cdot\colon F \times F \to F$ is such that $(F \setminus 0, \cdot)$ is an abelain group, where 0 is the additive identity.
(c) $a \cdot (b + c) = a \cdot b + a \cdot c$ for any $a, b, c \in F$.

Corollary 10.0.2. *Let $(F, +, \cdot)$ be a field. Then it is also a ring with the same additive and multiplicative identities.*

Definition 10.0.3 (Subfields)**.** Let K be a field and $F \subseteq K$. Then K is called a subfield of K iff the field operations of K can be inherited to F such that F is itself a field under those inherited operations.

We also call K a field extension of F, and this is denoted by K/F or

$$\begin{array}{c} K \\ | \\ F \end{array} .$$

Proposition 10.0.4 (A characterization of subfields)**.** *Let K be a field and $F \subseteq K$. Then F is a subfield of $K \iff F$ is an additive subgroup of K and $F \setminus \{0\}$ is a multiplicative subgroup of $K \setminus \{0\}$.*

Corollary 10.0.5.

(a) A subfield of a subfield is a subfield of the parent ring.
(b) Intersection of subrings is a subring.

Corollary 10.0.6 (Some examples)**.**

(a) $\mathbb{Z}/\mathbb{Z}p$ *is a finite field for any prime* $p \in Z$*.*

(b) $\mathbb{C}/\mathbb{R}/\mathbb{Q}$ *are field extensions.*

Definition 10.0.7 (Adjoining elements to a field)**.** Let K/F be a field extension and $\alpha \in K$. Then the smallest subfield of K containing F and α is denoted by $F(\alpha)$. We can extend this definition to any subset $S \subseteq K$ in place of α.

Proposition 10.0.8 (Description of $F(\alpha)$)**.** *Let* K/F *be a field extension and* $\alpha \in K$*. Then*

$$F(\alpha) = \{ f(\alpha)/q(\alpha) : f, g \in F[x] \text{ with } g(\alpha) \neq 0 \}.$$

Corollary 10.0.9. *Let* K/F *be a field extension and* $\alpha \in K$*. Then*

(a) $\alpha \in F \implies F(\alpha) = F$*, and*

(b) $\alpha \notin F \implies F(\alpha) \supsetneq F$*.*

Remark 10.0.10. We can extend Definition 10.0.7 to any subset $S \subseteq K$ in place of α, and then an analogue of Proposition 10.0.8 holds.

Proposition 10.0.11. *Let* K/F *be a field extension and* $\alpha, \beta \in K$*. Then* $F(\alpha, \beta) = F(\alpha)(\beta)$*.*

Chapter 11

Algebraics and transcendentals

March 17, 2022

Definition 11.0.1 (Algebraics and transcendentals)**.** Let K/F be a field extension and $\alpha \in K$. Then α is called

(a) algebraic over F iff there exists an $f \in F[x] \setminus 0$ such that $f(\alpha) = 0$, and
(b) transcendental over F iff it is not algebraic over F.

Remark 11.0.2. We might also call "$\alpha \in K/F$ is algebraic", or similar variants.

Corollary 11.0.3 (Some examples)**.**

(a) $i \in \mathbb{C}/\mathbb{R}$, $\sqrt{2} \in \mathbb{R}/\mathbb{Q}$ *are algebraic.*
(b) $\pi, e \in \mathbb{R}/\mathbb{Q}$ *are transcendental.* *Prove sometime...*
(c) $\sqrt{2} + \sqrt{3} \in \mathbb{R}/\mathbb{Q}$ *is algebraic. Further, it is irrational.*

Theorem 11.0.4 (When is $F[\alpha]$ a field?)**.** *Let K/F be a field extension and $\alpha \in K$. Consider the ring homomorphism*

$$\begin{aligned} \phi_\alpha \colon F[x] &\to K \\ f &\mapsto f(\alpha) \end{aligned}.$$

Then exactly one of the following holds:

(a) α *is algebraic over* F, $\ker \phi \neq \{0\}$, *and* $F[\alpha] = F(\alpha)$, *and*
(b) α *is transcendental over* F, $\ker \phi = \{0\}$, *and* $F[\alpha] \cong F[x]$.

Corollary 11.0.5. *We have the proper field extensions:* $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$.

Corollary 11.0.6. *Let* K/F *be a field extension and* $\alpha, \beta \in K/F$ *be transcendental. Then* $F[\alpha] \cong F[\beta]$.

Proposition 11.0.7 ($\ker\phi_\alpha$ when α is algebraic)**.** *Let $\alpha \in K/F$ be algebraic and $f \in F[x]$. Then the following are equivalent:*

(a) $\ker\phi_\alpha = (f)$.

(b) $f(\alpha) = 0$ *and* f *is irreducible in* $F[x]$.

Proposition 11.0.8 (Irreducible polynomial of an algebraic)**.** *Let $\alpha \in K/F$ be algebraic. Then there exists a unique monic irreducible polynomial $f \in F[x]$ such that $f(\alpha) = 0$.*

Definition 11.0.9 (Degree of an algebraic)**.** Let $\alpha \in K/F$ be algebraic. Then its degree, denoted $\deg_{K/F}\alpha$ is defined to be the degree of its irreducible polynomial.

Lemma 11.0.10. *Let $\alpha \in K/F$ be algebraic. Then $\deg_{K/F}\alpha \geq 1$ with equality holding if and only if $\alpha \in F$.*

Chapter 12

Degree of field extensions

March 18, 2022

Definition 12.0.1 (Degree of a field extension)**.** Let K/F be a field extension. Then K is a vector space over F with the operations inherited from K. Then the dimension of this vector space is called the degree of K/F, and is denoted by $[K : F]$.

Theorem 12.0.2 (Degree of $F(\alpha)/F$)**.** *Let $\alpha \in K/F$. Then we have the following disjoint cases:*

(a) α is algebraic and $\deg_{F(\alpha)/F} \alpha = [F(\alpha) : F]$, and $\{1, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ where $n := \deg_{F(\alpha)/F} \alpha$.
(b) α is transcendental and $[F(\alpha) : F] = \infty$ and $\{1, \alpha, \alpha^2, \ldots\}$ is an infinite independent set in $F(\alpha)$.

Corollary 12.0.3. *Let $\alpha \in K/F$. Then the following are equivalent:*

(a) α is algebraic.
(b) $[F(\alpha) : F] < \infty$.
(c) $F[\alpha]$ as a vector space over F has finite dimension.

Remark 12.0.4. We'll adopt the intuitive treatment of ∞.

Theorem 12.0.5 (Degree of fields is multiplicative)**.** *Let $K/L/F$ be field extensions. Then*

$$[K : F] = [K : L][L : F].$$

Also, we have the following disjoint cases:

(a) One of $[K : L]$ or $[L : F]$ is ∞ and $[K : F] = \infty$.
(b) $[K : L] = m$ and $[L : F] = n$ with $m, n < \infty$ and for any bases $(\alpha_1, \ldots, \alpha_m)$ and $(\beta_1, \ldots, \beta_n)$ of K over L and L over F respectively, the set $\{\alpha_i\beta_j\}_{i,j}$ is a basis for K over F.

12.1 Degree of $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$

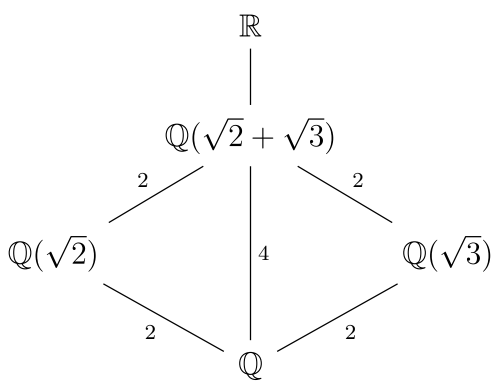
March 19, 2022

Proposition 12.1.1 ($\sqrt{2}+\sqrt{3} \in \mathbb{R}/\mathbb{Q}$ is algebraic)**.** *$\sqrt{2}+\sqrt{3}$ is a root of the polynomial $f \in \mathbb{Q}[x]$ given by*

$$x \mapsto x^4 - 10x^2 + 1.$$

Lemma 12.1.2. *Let K/F be a field extension such that $[K : F] = 1$. Then $K = F$.*

Proposition 12.1.3.



Corollary 12.1.4. *$x \mapsto x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$*

12.2 Field of algebraics

March 19, 2022

Definition 12.2.1 (Algebraic and finite extensions)**.** Let K/F be a field extension. Then K/F is called

(a) algebraic iff every $\alpha \in K/F$ is algebraic, and
(b) finite iff $[K : f] < \infty$.

Proposition 12.2.2. *Finite field extensions are algebraic.*

Remark 12.2.3. The converse need not be true. *Produce a counterexample.*

Theorem 12.2.4 (Algebraics of a field extension form a field)**.** *Let K/L be a field extension and $\alpha, \beta \in K/F$ be algebraic. Then $K/F(\alpha, \beta)/F$ are finite extensions.*

In particular, if L is the set of all algebraics in K/F, then

$$\begin{array}{c} K \\ | \\ L \\ | \\ F \end{array} .$$

Chapter 13

Field homomorphisms

March 21, 2022

Definition 13.0.1 (Field homomorphisms and isomorphisms)**.** Let K and L be fields. Then a ring homomorphism (respectively isomorphism) between them is called a field homomorphism (respectively isomorphism).

Remark 13.0.2. The condition that $1 \mapsto 1$ ensure that the zero map can't be a field homomorphism.

Corollary 13.0.3. *Field homomorphisms are injective.*

Definition 13.0.4 (F-homomorphisms and F-isomorphisms)**.** Let K/F and L/F be field extensions. Then a field homomorphism (respectively isomorphism) from K to L whose restriction to F is identity, is called an F-homomorphism (respectively F-isomorphism).

Corollary 13.0.5. *Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be field extensions. Then any field homomorphism from K to L is also a $\mathbb{Q}$-homomorphism.*

Proposition 13.0.6. *Let K/F and L/F be field extensions and $\alpha \in K/F$ be algebraic. Let $\phi\colon K \to L$ be an F-homomorphism. Then $\phi(\alpha) \in L/F$ is algebraic and has the same irreducible polynomial as α.*

Proposition 13.0.7. *Let K/F and L/F be field extensions and $\alpha \in K/F$ and $\beta \in L/F$ be algebraic with the same irreducible polynomial. Then there exists an F-isomorphism between $F(\alpha)$ and $F(\beta)$.*

Proposition 13.0.8. *Let $\alpha \in L/F$ be algebraic and $f \in F[x]$ be the irreducible polynomial of α. Let K be a field and $\phi\colon F \to K$ be a field homomorphism. Let $g \in K[x]$ be obtained by replacing the coefficients in F by their images under ϕ. Let $\beta \in K$ be a root of g. Then we can extend ϕ to a homomorphism $F(\alpha) \to K$ such that $\alpha \mapsto \beta$.*

$$\begin{array}{ccc} F[x] & \longrightarrow & K \\ {\scriptstyle \phi_\alpha}\big\downarrow & \searrow & \big\uparrow \\ F(\alpha) = F[\alpha] & \overset{\sim}{\longleftrightarrow} & F[x]/(f) \end{array}$$

Proposition 13.0.9. *There are exactly* 6 $\mathbb{Q}$*-self-homomorphisms on* $\mathbb{Q}(\sqrt[3]{2}, \omega)$.