Contents

% Created 2020-07-07 09:17 % Intended LaTeX compiler: pdflatex [11pt]article [utf8]inputenc [T1]fontenc graphicx grffile longtable wrapfig rotating [normalem]ulem amsmath textcomp amssymb capt-of hyperref minted

[dvipsnames]xcolor

forest qtree/.style= baseline, for tree= parent anchor=south, child anchor=north, align=center, inner sep=1pt,

[utf8]inputenc mathtools pgfplots amsthm amsmath

commath amssymb mathrsfs mathabx stmaryrd empheq pgfplots tikz tikz-cd arrows.meta,positioning,calc,fadings,decorations [most]tcolorbox threeparttable scalerel,stackengine stackrel tabularx dsfont [B1,T1]fontenc

enumitem siunitx subcaption caption auncial nosep float

fancyhdr [R]

unicode-math TeX Gyre Pagella Libertinus Math [range=„ „,]texgyrepa math.otf [range=⇉, ↠]$XITSMath[range = \int]LibertinusMath$

ifthen xargs

imakeidx othercode= [columns=2,options=-s /media/wu/file/stuuudy/notes/index$_style.ist, intoc$]

hyperref

definition plain definition remark Remark soul

largesymbols"62

graphicx

x z a k s h c o U L V v p I M N K t b A X u S Z y w T F m W R C D E Q P Y H B G

CL sg trdeg

cf ZFC

type **ZF**

im

Inn **AC** cod dom ran d d id LT Mat Eq irr Fr Gal lcm alg Th DLO DAG ODAG largesymbolsAUtxexamn *largesymbolsA*16

Ab Alg Rng Sets Met Aut R-**Mod** R-**Alg** LF op Diag el depth FO fin qr Mod TC Part Tot graph Fin Cof lh ord Idem z.div Frac rad nil Ann End coim coker Bil

mathxUmathxmn 1mathx"91 mathaUmathamn 2matha"63

{ pdfauthor={Atiyah \ Macdonald}, pdftitle={Introduction To Commutative Algebra}, pdfkeywords={}, pdfsubject={}, pdfcreator={Emacs

26.3 (Org mode 9.4)}, pdflang={English}}

Introduction To Commutative Algebra

Atiyah & Macdonald

July 7, 2020

Contents

1 Rings and Ideals

A **unit** is an element u with a **reciprocal** $1/u$ or the **multiplicative inverse**. The units form a multiplicative group, denoted $R^\times$

A ring **homomorphism**, or simply a **ring map**, $\varphi : R \to R'$ is a map preserving sum, products and 1

If there is an unspecified isomorphism between rings R and R', then we write $R = R'$ when it is **canonical**; that is, it does not depend on any artificial choices.

A subset $R'' \subset R$ is a **subring** if R'' is a ring and the inclusion $R'' \hookrightarrow R$

is a ring map. In this case, we call R a **(ring) extension**.

An R**-algebra** is a ring R' that comes equipped with a ring map $\varphi : R \to R'$, called the **structure map**, denoted by R'/R. For example, every ring is canonically a $\mathbb{Z}$-algebra. An R**-algebra homomorphism**, or R**-map**, $R' \to R''$ is a ring map between R-algebras.

A group G is said to **act** on R if there is a homomorphism given from G into the group of automorphism of R. The **ring of invariants** R^G is the subring defined by

$$R^G := \{x \in R \mid gx = g \text{ for all } g \in G\}$$

Similarly a group G is said to **act** on R'/R if G acts on R' and each

$g \in G$ is an R-map. Note that R'^G is an R-subalgebra

Boolean rings

The simplest nonzero ring has two elements, 0 and 1. It's denoted $\mathbb{F}_2$

Given any ring R and any set X, let R^X denote the set of functions

$f : X \to R$. Then R^X is a ring.

For example, take $R := \mathbb{F}_2$. Given $f : X \to R$, put $S := f^{-1}\{1\}$. Then

$f(x) = 1$ if $x \in S$. In other words, f is the **characteristic function** χ_S.

Thus *the characteristic functions form a ring, namely,* $\mathbb{F}_2^X$

Given $T \subset X$, clearly $\chi_S \cdot \chi_T = \chi_{S\cap T}$. $\chi_S + \chi_T = \chi_{S\triangle T}$, where $S\triangle T$ is the **symmetric difference**:

$$S \triangle T := (S \cup T) - (S \cap T)$$

Thus *the subsets of* X *form a ring: sum is symmetric difference, and product is intersection. This ring is canonically isomorphic to* $\mathbb{F}_2^X$

A ring B is called **Boolean** if $f^2 = f$ for all $f \in B$. If so, then $2f = 0$ as $2f = (f+f)^2 = f^2 + 2f + f^2 = 4f$

Suppose X is a topological space, and give $\mathbb{F}_2$ the **discrete** topology; that is, every subset is both open and closed. Consider the continuous functions $f : X \to \mathbb{F}_2$. Clearly, they are just the χ_S where S is both open and closed.

Polynomial rings

Let R be a ring, $P := R[X_1, \ldots, X_n]$. P has this **Universal Mapping Property** (UMP): *given a ring map $\varphi : R \to R'$ and given an element x_i of R' for each i, there is a unique ring map $\pi : P \to R'$ with $\pi|R = \varphi$ and $\pi(X_i) = x_i$.* In fact, since π is a ring map, necessarily π is given by the formula:

$$\pi(\sum a_{(i_1,\ldots,i_n)} X_1^{i_1} \ldots X_n^{i_n}) = \sum \varphi(a_{(i_1,\ldots,i_n)}) x_1^{i_1} \ldots x_n^{i_n} \tag{1.0.1}$$

In other words, P is universal among R-algebras equipped with a list of n elements

Similarly let $\mathcal{X} := \{X_\lambda\}_{\lambda\in\Lambda}$ be any set of variables. Set $P' := R[\mathcal{X}]$; the elements of P' are the polynomials in any finitely many of the X_λ. P' has essentially the same UMP as P

Ideals

Let R be a ring. A subset $\mathfrak{a}$ is called an **ideal** if

1. $0 \in \mathfrak{a}$
2. whenever $a, b \in \mathfrak{a}$, also $a + b \in \mathfrak{a}$
3. whenever $x \in R$ and $a \in \mathfrak{a}$ also $xa \in \mathfrak{a}$

Given a subset $\mathfrak{a} \subset R$, by the ideal $\langle\mathfrak{a}\rangle$ that $\mathfrak{a}$ **generates**, we mean the smallest ideal containing $\mathfrak{a}$

All ideal containing all the a_λ contains any (finite) **linear combination** $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and almost all 0.

Given a single element a, we say that the ideal $\langle a \rangle$ is **principal**

Given a number of ideals $\mathfrak{a}_\lambda$, by their **sum** $\sum \mathfrak{a}_\lambda$ we mean the set of all finite linear combinations $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and $a_\lambda \in \mathfrak{a}_\lambda$

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, by the **transporter** of $\mathfrak{b}$ into $\mathfrak{a}$ we mean the set

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} \subset \mathfrak{a}\}$$

$(\mathfrak{a} : \mathfrak{b})$ is an ideal. Plainly,

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$$

Further, for any ideal $\mathfrak{c}$, the distributive law holds: $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$

Given an ideal fa, notice $\mathfrak{a} = R$ *if and only if* $1 \in \mathfrak{a}$. It follows that $\mathfrak{a} = R$ iff $\mathfrak{a}$ contains a unit.

Given a ring map $\varphi : R \to R'$, denote by $\mathfrak{a}R'$ or $\mathfrak{a}^e$ the ideal of R' generated by the set $\varphi(\mathfrak{a})$. We call it the **extension** of $\mathfrak{a}$

Given an ideal $\mathfrak{a}'$ of R', its preimage $\varphi^{-1}(\mathfrak{a}')$ is an ideal of R. We call $\varphi^{-1}(\mathfrak{a}')$ the **contraction** of $\mathfrak{a}'$ and sometimes denote it by $\mathfrak{a}'^c$

Residue rings

kernel $\ker(\varphi)$ is defined to be the ideal $\varphi^{-1}(0)$ of R

Let $\mathfrak{a}$ be an ideal of R. Form the set of cosets of $\mathfrak{a}$

$$R/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in R\}$$

$R/\mathfrak{a}$ is called the **residure ring** or **quotient ring** or **factor ring** of R

modulo $\mathfrak{a}$. From the **quotient map**

$$\kappa : R \to R/\mathfrak{a} \quad \text{by } \kappa x := x + \mathfrak{a}$$

The element $\kappa x \in R/\mathfrak{a}$ is called the **residue** of x.

If $\ker(\varphi) \supset \mathfrak{a}$, *then there is a ring map* $\psi : R/\mathfrak{a} \to R'$ *with* $\psi\kappa = \varphi$; that

is, the following diagram is commutative

$$\mathrm{R}[\mathrm{r},"\kappa"][dr,"\varphi"]R/\mathfrak{a}[d,"\psi"]$$

R'

by $\psi(x\mathfrak{a}) = \varphi(x)$. Then we only need to verify that ψ is a map

Conversely, *if* ψ *exists, then* $\ker(\varphi) \supset \mathfrak{a}$, *or* $\varphi\mathfrak{a} = 0$, *or* $\mathfrak{a}R' = 0$, since

$\kappa\mathfrak{a} = 0$

Further, *if* ψ *exists, then* ψ *is unique* as κ is surjective

Finally, as κ is surjective, *if* ψ *exists, then* ψ *is surjective iff* ψ *is so.* In addition, ψ *is injective iff* $\mathfrak{a} = \ker(\varphi)$. Hence ψ *is an isomorphism iff* φ *is surjective and* $\mathfrak{a} = \ker(\varphi)$. Therefore,

$$R/\ker(\varphi) \xrightarrow{\sim} (\varphi)$$

$R/\mathfrak{a}$ has UMP: $\kappa(\mathfrak{a}) = 0$, and given $\varphi : R \to R'$ s.t. $\varphi : R \to R'$ s.t. $\varphi(\mathfrak{a}) = 0$, there is a unique ring map $\psi : R/\mathfrak{a} \to R'$ s.t. $\psi\kappa = \varphi$. In other words, $R/\mathfrak{a}$ is universal among R-algebras R' s.t. $\mathfrak{a}R' = 0$

If $\mathfrak{a}$ is the ideal generated by elements a_λ,then the UMP can be usefully rephrased as follows: $\kappa(a_\lambda) = 0$ for all λ, and given $\varphi : R \to R'$ s.t. $\varphi(a_\lambda) = 0$ for all λ, there is a unique ring map $\psi : R/\mathfrak{a} \to R'$ s.t. $\psi\kappa = \varphi$

The UMP serves to determine $R/\mathfrak{a}$ up to unique isomorphism. Say R', equipped with $\varphi : R \to R'$ has the UMP too. $\kappa(\mathfrak{a}) = 0$ so there is a unique $\psi' : R' \to R/\mathfrak{a}$ with $\psi'\varphi = \kappa$. Then $\psi'\psi\kappa = \kappa$. Hence $\psi'\psi = 1$ by uniqueness. Thus ψ and ψ' are inverse isomorphism

R/a[dd,"1"][dl,"ψ"]

R[urr,"κ"][r, "φ"][drr, "κ"]R'[dr, "ψ'"]

R/a

Proposition 1.1 () *Let R be a ring, $P := R[X]$, $a \in R$ and $\pi : P \to R$ the R-algebra map defined by $\pi(X) := a$. Then*

1. $\ker(\pi) = \{F(X) \in P \mid F(a) = 0\} = \langle X - a \rangle$

2. $R/\langle X - a \rangle \simeq R$

Set $G := X - a$. Given $F \in P$, let's show $F = GH + r$ with $H \in P$ and $r \in R$. By linearity, we may assume $F := X^n$. If $n \geq 1$, then $F =$

$(G + a)X^{n-1}$, so $F = GH + aX^{n-1}$ with $H := X^{n-1}$.

Then $\pi(F) = \pi(G)\pi(H) + \pi(r) = r$. Hence $F \in \ker(\pi)$ iff $F = GH$. But

$\pi(F) = F(a)$ by **??**

Degree of a polynomial

Let R be a ring, P the polynomial ring in any number of variables. If F is

a monomial , then its degree deg() is the sum of its exponents; in general,

$\deg(F)$ is the largest deg() of all monomials in F

Given any $G \in P$ with FG nonzero, notice that

$$\deg(FG) \leq \deg(F) + \deg(G)$$

Order of a polynomial

Let R be a ring, P the polynomial ring in variable X_λ for $\lambda \in \Lambda$, and $(x_\lambda) \in R^\Lambda$ a vector. Let $\varphi_{(x_\lambda)} : P \to P$ denote the R-algebra map defined by $\varphi_{(x_\lambda)} X_\mu := X_\mu + x_\mu$ for all $\mu \in \Lambda$. Fix a nonzero $F \in P$

The **order** of F at the zero vector (0), denoted ${}_{(0)}F$, is defined as the smallest deg() of all the monomials in F. In general, the **order** of F at the vector (x_λ), denoted ${}_{(x_\lambda)}F$ is defined by the formula: ${}_{(x_\lambda)}F :={}_{(0)} (\varphi_{(x_\lambda)}F)$

Notice that ${}_{(x_\lambda)}F = 0$ iff $F(x_\lambda) \neq 0$ as $(\varphi_{x_\lambda}F)(0) = F(x_\lambda)$

Given μ and $x \in R$, form $F_{\mu,x}$ by substituting x for X_μ in F. If $F_{\mu,x_\mu} \neq 0$

, then

$$_{(x_\lambda)}F \leq_{(x_\lambda)} F_{\mu,x_\mu}$$

If $x_\mu = 0$, then F_{μ,x_μ} is the sum of the terms without x_μ in F. Hence if $(x_\lambda) = (0)$, then **??** holds. But substituting 0 for X_μ in $\varphi_{(x_\lambda)}F$ is the same as substituting x_μ for X_μ in F and then applying $\varphi_{(x_\lambda)}$ to the result; that is, $(\varphi_{(x_\mu)}F)_{\mu,0} = \varphi_{(x_\lambda)}F_{\mu,x_\mu}$

Given any $G \in P$ with FG nonzero,

$$_{(x_\lambda)}FG \geq_{(x_\lambda)} F +_{(x_\lambda)} G$$

Nested ideals

Let R be a ring, $\mathfrak{a}$ an ideal, and $\kappa : R \to R/\mathfrak{a}$ the quotient map. Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the corresponding set of cosets of $\mathfrak{a}$

$$\mathfrak{b}/\mathfrak{a} := \{b + \mathfrak{a} \mid b \in \mathfrak{b}\} = \kappa(\mathfrak{b})$$

Clearly, $\mathfrak{b}/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$. Also $\mathfrak{b}/\mathfrak{a} = \mathfrak{b}(R/\mathfrak{a})$

The operation $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ and $\mathfrak{b}' \mapsto \kappa^{-1}(\mathfrak{b}')$ are inverse to each other, and establish a bijective correspondence between the set of ideals $\mathfrak{b}$ of R containing $\mathfrak{a}$ and the set of all ideals $\mathfrak{b}'$ of $R/\mathfrak{a}$. Moreover, this correspondence preserves inclusions

Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the composition of the quotient maps

$$\varphi : R \to R/\mathfrak{a} \to (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$$

φ is surjective and $\ker(\varphi) = \mathfrak{b}$. Hence φ factors

R[r][d]R/b[d,"ψ”,” $\simeq$ ”′]

R/a[r](R/a)/(b/a)

Idempotents

Let R be a ring. Let $e \in R$ be an **idempotent**; that is, $e^2 = e$. Then Re is a ring with e as 1.

Set $e' := 1 - e$. Then e' is idempotent and $e \cdot e' = 0$. We call e and e' **complementary idempotents**. Conversely, if two elements $e_1, e_2 \in R$

satisfy $e_1 + e_2 = 1$ and $e_1 e_2 = 0$, then they are complementary idempotents,

as for each i,

$$e_i = e_i \cdot 1 = e_i(e_1 + e_2) = e_i^2$$

We denote the set of all idempotents by (R). Let $\varphi : R \to R'$ be a ring map.

Then $\varphi(e)$ is idempotent. So the restriction of φ to (R) is a map

$$(\varphi) : (R) \to (R')$$

Example 1.1 () *Let $R := R' \times R''$ be a* ***product*** *of two rings. Set $e' :=$ $(1, 0)$ and $e'' := (0, 1)$. Then e' and e'' are complementary idempotents.*

Proposition 1.2 () *Let R be a ring, and e', e'' complementary idempotents.*

Set $R' := Re'$ and $R'' := Re''$. Define $\varphi : R \to R' \times R''$ by $\varphi(x) := (xe', xe'')$.

Then φ is a ring isomorphism. Moreover, $R' = R/Re''$ and $R'' = R/Re'$

Define a surjection $\varphi' : R \to R'$ by $\varphi'(x) := xe'$. Then φ' is a ring map, since $xye' = xye'^2 = (xe')(ye')$. Moreover, $\ker(\varphi') = Re''$ since $x = x \cdot 1 = xe' + xe'' = xe''$. Thus $R' = R/Re''$

Since φ is a ring map. It's surjective since $(xe', x'e'') = \varphi(xe' + x'e'')$

Exercise

Exercise 1.0.1 *Let $\varphi : R \to R'$ be a map of rings, $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}$ ideals of R, $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}$ ideals of R'. Prove*

1. $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$

2. $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c + \mathfrak{b}_2^c$

3. $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subset \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$

4. $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$

5. $(\mathfrak{a}_1 \mathfrak{a}_2)^e = \mathfrak{a}_1^e \mathfrak{a}_2^e$

6. $(\mathfrak{b}_1 \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c \mathfrak{b}_2^c$

7. $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subset (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$

8. $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subset (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$

Exercise 1.0.2 *Let $\varphi : R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$*

an ideal of R'. Prove the following statements:

1. $\mathfrak{a}^{ec} \supset \mathfrak{a}$ *and* $\mathfrak{b}^{ce} \subset \mathfrak{b}$

2. $\mathfrak{a}^{ece} = \mathfrak{a}^{e}$ *and* $\mathfrak{b}^{cec} = \mathfrak{b}^{c}$

3. *If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^{c}$ is the largest ideal of R with extension $\mathfrak{b}$*

4. *If two extensions have the same contraction, then they are equal*

Exercise 1.0.3 *Let R be a ring, $\mathfrak{a}$ an ideal, $\mathcal{X}$ a set of variables. Prove:*

1. *The extension $\mathfrak{a}(R[\mathcal{X}])$ is the set $\mathfrak{a}[\mathcal{X}]$*

2. $\mathfrak{a}(R[\mathcal{X}]) \cap R = \mathfrak{a}$

Exercise 1.0.4 *Let R be a ring, $\mathfrak{a}$ an ideal, and $\mathcal{X}$ a set of variables. Set $P := R[\mathcal{X}]$. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[\mathcal{X}]$*

Exercise 1.0.5 *Let R be a ring, $P := R[\{X_\lambda\}]$ the polynomial ring in variables X_λ for $\lambda \in \Lambda$ a vector. Let $\pi_{(x_\lambda)} : P \to R$ denote the R-algebra map defined by $\pi_{(x_\lambda)} X_\mu := x_\mu$ for all $\mu \in \Lambda$. Show:*

1. *Any $F \in P$ has the form $F = \sum a_{(i_1,\ldots,i_n)}(X_{\lambda_1}^{i_1} - x_{\lambda_1}) \ldots (X_{\lambda_n} - x_{\lambda_n})^{i_n}$ for unique $a_{(i_1,\ldots,i_n)} \in R$*

2. $\ker(\pi_{(x_\lambda)}) = \{F \in P \mid F((x_\lambda)) = 0\} = \langle\{X_\lambda - x_\lambda\}\rangle$

3. *π induces an isomorphism $P/\langle\{X_\lambda - x_\lambda\}\rangle \simeq R$*

4. *Given $F \in P$, its residue in $P/\langle\{X_\lambda - x_\lambda\}\rangle$ is equal to $F((x_\lambda))$*

5. *Let $\mathcal{Y}$ be a second set of variables. Then $P[\mathcal{Y}]/\langle\{X_\lambda - x_\lambda\}\rangle \simeq R[\mathcal{Y}]$*

1. Let $\varphi_{(x_\lambda)}$ be the R-automorphism of P. Say $\varphi_{(x_\lambda)}F = \sum a_{(i_1,\ldots,i_n)}X_{\lambda_1}^{i_1}\ldots X_{\lambda_n}^{i_n}$

   . And $\varphi_{(x_\lambda)}^{-1}\varphi_{(x_\lambda)}F = F$

2. Note that $\pi_{(x_\lambda)}F = F((x_\lambda))$. Hence $F \in \ker(\pi_{(x_\lambda)})$ iff $F((x_\lambda)) = 0$. If

   $F((x_\lambda)) = 0$, then $a_{(0,\ldots,0)} = 0$, and so $F \in \langle\{X_\lambda - x_\lambda\}\rangle$

5. Set $R' := R[\mathcal{Y}]$

Exercise 1.0.6 *Let R be a ring, $P := R[X_1,\ldots,X_n]$ the polynomial ring* *in variables* X_i*. Given* $F = \sum a_{(i_1,\ldots,i_n)} X_1^{i_1} \ldots X_n^{i_n} \in P$*, formally set*

$$\partial F/\partial X_j := \sum i_j a_{(i_1,\ldots,i_n)} X_1^{i_i} \ldots X_n^{i_n}/X_j \in P$$

Given $(x_1, \ldots, x_n) \in R^n$*, set* $:= (x_1, \ldots, x_n)$*, set* $a_j := (\partial F/\partial X_j)()$*, and set* $\mathfrak{M} := \langle X_1 - x_1, \ldots, X_n - x_n \rangle$*. Show* $F = F() + \sum a_j (X_j - x_j) + G$ *with* $G \in \mathfrak{M}^2$*. First show that if* $F = (X_1 - x_1)^{i_1} \ldots (X_n - x_n)^{i_n}$*, then*

$\partial F/\partial X_j = i_j F/(X_j - x_j)$

$(\partial F/\partial X_j)() = b_{(\delta_{1j},\ldots,\delta_{nj})}$ where δ_{ij} is the Kronecker delta

Exercise 1.0.7 *Let* R *be a ring,* X *a variable,* $F \in P := R[x]$*, and* $a \in R$*. Set* $F' := \partial F/\partial X$*. We call* a *a* ***root*** *of* F *if* $F(a) = 0$*, a* ***simple root*** *if also*

$F'(a) \neq 0$, *and a* ***supersimple root*** *if also* $F'(a)$ *is a unit.*

Show that a *is a root of* F *iff* $F = (X-a)G$ *for some* $G \in P$*, and if so, then* G *is unique; that* a *is a simple root iff also* $G(a) \neq 0$*; and that* a *is a supersimple root iff also* $G(a)$ *is a unit*

Exercise 1.0.8 *Let* R *be a ring,* $P := R[X_1, \ldots, X_n]$*,* $F \in P$ *of degree* d *and* $F_i := X_i^{d_i} + a_1 X_i^{d_i - 1} + \ldots$ *a monic polynomial in* X_i *aloen for all* i*. Find* $G, G_i \in P$ *s.t.* $F = \sum_{i=1}^{n} F_i G_i + G$ *where* $G_i = 0$ *or* $deg(G_i) \leq d - d_i$ *and where the highest power of* X_i *in* G *is less than* d_i

By linearity, we may assume $F := X_1^{m_1} \ldots X_n^{m_n}$. If $m_i < d_i$ for all i, set $G_i := 0$ and $G := F$ and we're done. Else, fix i with $m_i \geq d_i$, and set

$G_i := F/X_i^{d_i}$ and $G := (-a_1 X_i^{d_i-1} - \dots)G_i$

Exercise 1.0.9 (Chinese Remainder Theorem) *Let R be a ring*

1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be **comaximal** ideals; that is, $\mathfrak{a} + \mathfrak{b} = R$. Show*

   (a) $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$

   (b) $R/\mathfrak{a}\mathfrak{b} = (R/\mathfrak{a}) \times (R/\mathfrak{b})$

2. *Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Show $\mathfrak{a}$ is also comaximal to $\mathfrak{b}\mathfrak{b}'$*

3. *Given $m, n \geq 1$, show $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal iff $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are.*

4. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pairwise comaximal. Show*

(a) $\mathfrak{a}_1$ *and* $\mathfrak{a}_2 \ldots \mathfrak{a}_n$ *are comaximal*

(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \ldots \mathfrak{a}_n$

(c) $R/(\mathfrak{a}_1 \ldots \mathfrak{a}_n) \simeq \prod(R/\mathfrak{a}_i)$

5. *Find an example where* $\mathfrak{a}$ *and* $\mathfrak{b}$ *satisfy 1.1 but aren't comaximal*

1. $\mathfrak{a} + \mathfrak{b} = R$ implies $x + y = 1$ with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. So given $z \in \mathfrak{a} \cap \mathfrak{b}$,

   we have $z = xz + yz \in \mathfrak{a}\mathfrak{b}$

2. $R = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{b}') = (\mathfrak{a}^2 + \mathfrak{b}\mathfrak{a} + \mathfrak{a}\mathfrak{b}') + \mathfrak{b}\mathfrak{b}' \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{b}' \subseteq R$

3. Build with $\mathfrak{a} + \mathfrak{b}^2 = R$. Conversely, note that $\mathfrak{a}^n \subset \mathfrak{a}$

4. Induction

5. Let k be a field. Take $R := k[X, Y]$ and $\mathfrak{a} := \langle X \rangle$ and $\mathfrak{b} := \langle Y \rangle$. Given $f \in \langle X \rangle \cap \langle Y \rangle$, note that every monomial of f contains both X and Y, and so $f \in \langle X \rangle \langle Y \rangle$. But $\langle X \rangle$ and $\langle Y \rangle$ are not comaximal

Exercise 1.0.10 *First given a prime number p and a $k \geq 1$, find the idempotents in $\mathbb{Z}/\langle p^k \rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12 \rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n \rangle$ where $n = \prod_{i=1}^{N} p_i^{n_i}$ with p_i distinct prime numbers*

$x = 0, 1$

Since $-3+4=1$, the Chinese Remainder Theorem yields

$$\mathbb{Z}/\langle 12\rangle = \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 4\rangle$$

m is idempotent in $\mathbb{Z}/\langle 12\rangle$ iff it's idempotent in $\mathbb{Z}/\langle 3\rangle$ and $\mathbb{Z}/\langle 4\rangle$

$p_i^{n_i}$ has a linear combination equal to 1. Hence 2^N

Exercise 1.0.11 *Let* $R := R' \times R''$ *be a product of rings,* $\mathfrak{a} \subset R$ *an ideal.*

Show $\mathfrak{a} = \mathfrak{a}' \times \mathfrak{a}''$ *with* $\mathfrak{a}' \subset R$ *and* $\mathfrak{a}'' \subset R''$ *ideals. Show* $R/\mathfrak{a} = (R'/\mathfrak{a}') \times$

$(R''/\mathfrak{a}'')$

Exercise 1.0.12 *Let* R *be a ring;* e, e' *idempotents. Show*

1. *Set* $\mathfrak{a} := \langle e\rangle$*. Then* $\mathfrak{a}$ *is idempotent; that is,* $\mathfrak{a}^2 = \mathfrak{a}$

2. *Let $\mathfrak{a}$ be a principal idempotent ideal. Then $\mathfrak{a} = \langle f \rangle$ with f idempotent*

3. *Set $e'' := e + e' - ee'$. Then $\langle e, e' \rangle = \langle e'' \rangle$ and e'' is idempotent*

4. *Let $e_1, \ldots, e_r$ be idempotents. Then $\langle e_1, \ldots, e_r \rangle = \langle f \rangle$ with f idempotent*

5. *Assume R is Boolean. Then every finitely generated ideal is principal*

3. $ee'' = e^2 = e$

Exercise 1.0.13 *Let L be a **lattice**, that is, a partially ordered set in which every pair $x, y \in L$ has a sup $x \vee y$ and an inf $x \wedge y$. Assume L is **Boolean;** that is:*

1. *L has a least element 0 and a greatest element 1*

2. *The operations* $\vee$ *and* $\wedge$ ***distribute*** *over each other*

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \textit{and} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

3. *Each* $x \in L$ *has a unique* ***complement*** x'*; that is,* $x \wedge x' = 0$ *and*

$x \vee x' = 1$.

Show that the following six laws obeyed

$$\begin{array}{rcll}
x \wedge x = x & \textit{and} & x \vee x = x & \textbf{\textit{(idempotent)}} \\
x \wedge 0 = 0, x \wedge 1 = x & \textit{and} & x \vee 1 = 1, x \vee 0 = x & \textbf{\textit{(unitary)}} \\
x \wedge y = y \wedge x & \textit{and} & x \vee y = y \vee x & \textbf{\textit{(commutative)}} \\
x \wedge (y \wedge z) = (x \wedge y) \wedge z & \textit{and} & x \vee (y \vee z) = (x \vee y) \vee z & \textbf{\textit{(associative)}} \\
x'' = x & \textit{and} & 0' = 1, 1' = 0 & \textbf{\textit{(involutory)}} \\
(x \wedge y)' = x' \vee y' & \textit{and} & (x \vee y)' = x' \wedge y' & \textbf{\textit{(De Morgan's)}}
\end{array}$$

Moreover, show that $x \leq y$ *iff* $x = x \wedge y$

Exercise 1.0.14 *Let L be a Boolean lattice. For all $x, y \in L$, set*

$$x + y := (x \wedge y') \vee (x' \wedge y) \quad \text{and} \quad xy := x \wedge y$$

Show

1. $x + y = (x \vee y)(x' \vee y')$
2. $(x + y)' = (x'y') \vee (xy)$
3. *L is a Boolean ring*

Exercise 1.0.15 *Given a Boolean ring R, order R by $x \leq y$ if $x = xy$. Show R is thus a Boolean lattice. Viewing this construction as a map ρ from the set of Boolean-ring structures on the set R to the set of Boolean-*

lattice structures on R, show ρ is bijective with inverse the map λ associated to the construction in **??**

First check R is partially ordered.

Given $x, y \in R$, set $x \vee y := x + y + xy$ and $x \wedge y := xy$. Then $x \leq x \vee y$ as $x(x + y + xy) = x^2 + xy + x^2y = x + 2xy = x$. If $z \leq x$ and $z \leq y$, then $z = zx$ and $z = zy$, and so $z(x \vee y) = z$; thus $z \leq x \vee y$

Exercise 1.0.16 *Let X be a set, and L the set of all subsets of X, partially ordered by inclusion. Show that L is a Boolean lattice and that the ring structure on L constructed in* **??** *coincides with that constructed in* **??**

Assume X is a topological space, and let M be the set of all its open and closed subsets. Show that M is a sublattice of L, and that the subring structure on M of **??** *coincides with the ring structure of* **??** *with M for L*

2 Prime Ideals

Zerodivisors

Let R be a ring. An element x is called a **zerodivisor** if there is a nonzero y with $xy = 0$; otherwise x is called a **nonzerodivisor**. Denote the set of zerodivisors by (R) and the set of nonzerodivisor by S_0

Multiplicative subsets, prime ideals

Let R be a ring. A subset S is called **multiplicative** if $1 \in S$ and if $x, y \in S$ implies $xy \in S$

An ideal $\mathfrak{p}$ is called **prime** if its complement $R - \mathfrak{p}$ is multiplicative, or equivalently, if $1 \notin \mathfrak{p}$ and if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

Fields, domains

A ring is called a **field** if $1 \neq 0$ and if every nonzero element is a unit.

A ring is called an **integral domain**, or simply a **domain**, if $\langle 0 \rangle$ is prime, or equivalently, if R is nonzero and has no nonzero zerodivisors.

Every domain R is a subring of its **fraction field** (R). Conversely, any subring R of a field K, including K itself, is a domain. Further, (R) has this UMP: the inclusion of R into any field L extends uniquely to an inclusion of (R) into L.

Polynomials over a domain

Let R be a domain, $\mathcal{X} := \{X_\lambda\}_{\lambda\in\Lambda}$ a set of variables. Set $P := R[\mathcal{X}]$. Then P is a domain too. In fact, given nonzero $F, G \in P$, not only is their product FG nonzero, but also given a well ordering of the variables, the grlex leading term of FG is the product of the grlex leading terms of F and G, and

$$\deg(FG) = \deg(F) + \deg(G)$$

Using the given ordering of the variables, well order all the monomials of the same degree via the lexicographic order on exponents. Among the in F with $\deg() = \deg(F)$, the largest is called the **grlex leading monomial** (graded lexicographic) of F. Its **grlex leading term** is the product a whre $a \in R$

is the coefficient of in F, and a is called the **grlex leading coefficient**

The grlex leading term of FG is the product of those a and b of F and G. and **??** holds, for the following reasons. First, $ab \neq 0$ as R is domain.

Second

$$\deg() = \deg() + \deg() = \deg(F) + \deg(G)$$

Third, $\deg() \geq \deg('')$ for every pair of monomials $'$ and $'$ in F and G.

The grlex hind term of FG is the product of the grlex hind terms of F and G. Further, given a vector $(x_\lambda) \in R^\Lambda$, then

$$_{(x_\lambda)}FG =_{(x_\lambda)} F +_{(x_\lambda)} G$$

Among the monomials in F with $() = (F)$, the smallest is called the **grlex hind monomial** of F. The **grlex hind term** of F os the product a where $a \in R$ is the coefficient of in F

The fraction field (P) is called the field of **rational functions**, and is also denoted by $K(\mathcal{X})$ where $K := (R)$

Unique factorization

Let R be a domain, p a nonzero nonunit. We call p **prime** if whenever $p \mid xy$, either $p \mid x$ or $p \mid y$. *p is prime iff $\langle p \rangle$ is prime*

We call p **irreducible** if whenever $p = yz$, either y or z is a unit. We call R a **Unique Factorization Domain** (UFD) if

1. every nonzero nonunit factors into a product of irreducibles

2. the factorization is unique up to order and units.

If R is a UFD, then $\gcd(x, y)$ always exists

Lemma 2.1 () *Let $\varphi : R \to R'$ be a ring map, and $T \subset R'$ a subset. If T is multiplicative, then $\varphi^{-1}T$ is multiplicative; the converse holds if φ is surjective*

Proposition 2.2 () *Let $\varphi : R \to R'$ be a ring map, and $\mathfrak{q} \subset R'$ an ideal. Set $\mathfrak{p} := \varphi^{-1}\mathfrak{q}$. If $\mathfrak{q}$ is prime, then $\mathfrak{p}$ is prime; the converse holds if φ is surjective*

Corollary 2.3 () *Let R be a ring, $\mathfrak{p}$ an ideal. Then $\mathfrak{p}$ is prime iff $R/\mathfrak{p}$ is a domain*

By Proposition **??**, $\mathfrak{p}$ is prime iff $\langle 0 \rangle \subset R/\mathfrak{p}$ is

Exercise 2.0.1 *Let R be a ring, $P := R[\mathcal{X}, \mathcal{Y}]$ the polynomial ring in two sets of variables $\mathcal{X}$ and $\mathcal{Y}$. Set $\mathfrak{p} := \langle \mathcal{X} \rangle$. Show $\mathfrak{p}$ is prime iff R is a domain*

$\mathfrak{p}$ is prime iff $R[\mathcal{Y}]$ is a domain

Definition 2.4 () *Let R be a ring. An ideal $\mathfrak{m}$ is said to be* ***maximal*** *if $\mathfrak{m}$ is proper and if there is no proper ideal $\mathfrak{a}$ with $\mathfrak{m} \subsetneq \mathfrak{a}$*

Example 2.1 () *Let R be a domain, $R[X, Y]$ the polynomial ring. Then*

$\langle X \rangle$ is prime. However, $\langle X \rangle$ is not maximal since $\langle X \rangle \subsetneq \langle X, Y \rangle$

Proposition 2.5 () *A ring R is a field iff $\langle 0 \rangle$ is a maximal ideal*

If $\langle 0 \rangle$ is maximal. Take $x \neq 0$, then $\langle x \rangle \neq 0$. So $\langle x \rangle = R$ and x is a unit.

Corollary 2.6 () *Let R be a ring, $\mathfrak{m}$ an ideal. Then $\mathfrak{m}$ is maximal iff $R/\mathfrak{m}$ is a field.*

$\mathfrak{m}$ is maximal iff $\langle 0 \rangle$ is maximal in $R/\mathfrak{m}$ by Correspondence Theorem.

Example 2.2 () *Let R be a ring, P the polynomial ring in variable X_λ, and $x_\lambda \in R$ for all λ. Set $\mathfrak{m} := \langle \{X_\lambda - x_\lambda\} \rangle$. Then $P/\mathfrak{m} = R$ by Exercise*

??. *Thus $\mathfrak{m}$ is maximal iff R is a field*

Corollary 2.7 () *In a ring, every maximal ideal is prime*

Coprime elements

Let R be a ring and $x, y \in R$. We say x and y are **(strictly) coprime** if their ideals $\langle x\rangle$ and $\langle y\rangle$ are comaximal

Plainly, x and y are coprime iff there are $a, b \in R$ s.t. $ax + by = 1$

Plainly, x and y are coprime iff there is $b \in R$ with $by \equiv 1 \mod \langle x\rangle$ iff the residue of y is a unit in $R/\langle x\rangle$

Fix $m, n \geq 1$. By Exercise **??**, x and y are coprim eiff x^m and x^n are.

If x and y are coprime, then their images in algebra R' too.

PIDs

A domain R is called a **Principal Ideal Domain** (PID) if every ideal is principal. A PID is a UFD

Let R be a PID, $\mathfrak{p}$ a nonzero prime ideal. Say $\mathfrak{p} = \langle p \rangle$. Then p is prime, so irreducible. Now let $q \in R$ be irreducible. Then $\langle q \rangle$ is maximal for: if $\langle q \rangle \subsetneq \langle x \rangle$, then $q = xy$ for some nonunit y; so x must be a unit as q is irreducible. So $R/\langle q \rangle$ is a field. Also $\langle q \rangle$ is prime; so q is prime Thus every irreducible element is prime, and every nonzero prime ideal is maximal

Exercise 2.0.2 *Show that, in a PID, nonzero elements x and y are **rela-***

tively prime *(share no prime factor) iff they are coprime*

Say $\langle x\rangle + \langle y\rangle = \langle d\rangle$. Then $d = \gcd(x, y)$

Example 2.3 () *Let R be a PID, and $p \in R$ a prime. Set $k := R/\langle p\rangle$. Let X be a variable, and set $P := R[X]$. Take $G \in P$; let G' be its image in $k[X]$; assume G' is irreducible. Set $\mathfrak{m} := \langle p, G\rangle$. Then $P/\mathfrak{m} \simeq k[X]/\langle G'\rangle$ by* **??** *and* **??** *and $k[X]/\langle G'\rangle$ is a field; hence $\mathfrak{m}$ is maximal*

Theorem 2.8 () *Let R be a PID. Let $P := R[X]$ and $\mathfrak{p}$ a nonzero prime ideal of P*

1. *$\mathfrak{p} = \langle F\rangle$ with F prime or $\mathfrak{p}$ is maximal*

2. *Assume* $\mathfrak{p}$ *is maximal. Then either* $\mathfrak{p} = \langle F\rangle$ *with* F *prime, or* $\mathfrak{p} = \langle p, G\rangle$ *with* $p \in R$ *prime,* $pR = \mathfrak{p} \cap R$ *and* $G \in P$ *prime with image* $G' \in (R/pR)[X]$ *prime*

P is a UFD.

If $\mathfrak{p} = \langle F\rangle$ for some $F \in P$, then F is prime. Assume $\mathfrak{p}$ isn't principal

Take a nonzero $F_1 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathfrak{p}$ contains a prime factor F_1' of F_1. Replace F_1 by F_1'. As $\mathfrak{p}$ isn't principal, $\mathfrak{p} \neq \langle F_1\rangle$. So there is a prime $F_2 \in \mathfrak{p} - \langle F_1\rangle$. Set $K := (R)$, Gauss's lemma implies that F_1 and F_2 are also prime in $K[X]$. So F_1 and F_2 are relatively prime in $K[X]$. So **??** yield $G_1, G_2 \in P$ and $c \in P$ with $(G_1/c)F_1 + (G_2/c)F_2 = 1$. So

$c = G_1F_1 + G_2F_2 \in R \cap \mathfrak{p}$. Hence $R \cap \mathfrak{p} \neq 0$. But $R \cap \mathfrak{p}$ is prime, and R is a PID; so $R \cap \mathfrak{p} = pR$ where p is prime. Also pR is maximal.

Set $k := R/pR$. Then k is a field. Set $\mathfrak{q} := \mathfrak{p}/pR \subset k[X]$. Then $k[X]/\mathfrak{q} = P/\mathfrak{p}$ by **??**. But $\mathfrak{p}$ is prime, so $P/\mathfrak{p}$ is a domain. So $k[X]/\mathfrak{q}$ is a domain too. So $\mathfrak{q}$ is prime. So $\mathfrak{q}$ is maximal. So $\mathfrak{p}$ is maximal.

Since $k[X]$ is a PID and $\mathfrak{q}$ is prime, $\mathfrak{q} = \langle G' \rangle$ where G' is prime in $k[X]$. Take $G \in \mathfrak{p}$ with image G'

Theorem 2.9 () *Every proper ideal* $\mathfrak{a}$ *is contained in some maximal ideal*

Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \not\ni 1\}$. Then $\mathfrak{a} \in \mathcal{S}$ and $\mathcal{S}$ is partially ordered by inclusion. By Zorn's Lemma

Corollary 2.10 () *Let R be a ring, $x \in R$. Then x is a unit iff x belongs to no maximal ideal*

Exercise

Exercise 2.0.3 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent*

1. $\mathfrak{a} \subset \mathfrak{p}$ *or* $\mathfrak{b} \subset \mathfrak{p}$
2. $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$
3. $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$

Exercise 2.0.4 *Let R be a ring, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ maximal ideals. Assume $\mathfrak{m}_1 \dots \mathfrak{m}_n = 0$. Show $\mathfrak{p} = \mathfrak{m}_i$ for some i*

Note $\mathfrak{p} \supset 0 = \mathfrak{m}_1 \dots \mathfrak{m}_n$. So $\mathfrak{p} \supset \mathfrak{m}_1$ or $\mathfrak{p} \supset \mathfrak{m}_2 \dots \mathfrak{m}_n$ by **??**

Exercise 2.0.5 *Let R be a ring, and $\mathfrak{p}, \mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideals with $\mathfrak{p}$ prime*

1. *Assume $\mathfrak{p} \supset \bigcap_{i=1}^{n} \mathfrak{a}_i$. Show $\mathfrak{p} \supset \mathfrak{a}_j$ for some j*

2. *Assume $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$. Show $\mathfrak{p} = \mathfrak{a}_j$ for some j*

Exercise 2.0.6 *Let R be a ring, $\mathcal{S}$ the set of all ideals that consist entirely of zerodivisors. Show that $\mathcal{S}$ has maximal elements and they're prime. Conclude that (R) is a union of primes.*

Order $\mathcal{S}$ by inclusion. $\mathcal{S}$ is not empty. $\mathcal{S}$ consists of a maximal element $\mathfrak{p}$.

Given $x, x' \in R$ with $xx' \in \mathfrak{p}$, but $x, x' \notin \mathfrak{p}$. Hence $\langle x \rangle + \mathfrak{p}, \langle x' \rangle + \mathfrak{p} \notin \mathcal{S}$. So there are $a, a' \in R$ and $p, p' \in \mathfrak{p}$ s.t. $y := ax + p$ and $y' := a'x' + p'$ are not zerodivisors. Then $yy' \in \mathfrak{p}$. So $yy' \in (R)$, a contradiction. Thus $\mathfrak{p}$ is prime.

Given $x \in (R)$, note $\langle x \rangle \in \mathcal{S}$. So $\langle x \rangle$ lies in a maximal element $\mathfrak{p}$ of $\mathcal{S}$. Thus $x \in \mathfrak{p}$ and $\mathfrak{p}$ is prime

Exercise 2.0.7 *Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n \rangle$ does not contain a domain as a subring*

Any subring of $\mathbb{Z}/\langle p^n \rangle$ must contain 1, and 1 generates $\mathbb{Z}/\langle p^n \rangle$ as an Abelian group. So $\mathbb{Z}/\langle p^n \rangle$ contains no proper subrings.

Exercise 2.0.8 *Let $R := R' \times R''$ be a product of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other 0*

Assume R is a domain. As $(1,0) \cdot (0,1) = (0,0)$, either R' or R'' is 0.

Exercise 2.0.9 *Let $R := R' \times R''$ be a product of rings, $\mathfrak{p} \subset R$ an ideal. Show $\mathfrak{p}$ is prime iff either $\mathfrak{p} = \mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $\mathfrak{p} = R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime*

$1 \in \mathfrak{p}$. $(1,0)(0,1) \in \mathfrak{p}$. Hence $(1,0) \in \mathfrak{p}$ or $(0,1) \in \mathfrak{p}$.

Exercise 2.0.10 *Let R be a domain, and $x, y \in R$. Assume $\langle x \rangle = \langle y \rangle$.*

Show $x = uy$ for some unit u

$(1 - tu)y = 0$ and domain

Exercise 2.0.11 *Let k be a field, R a nonzero ring, $\varphi : k \to R$ a ring map.*

Prove φ is injective

Since $1 \neq 0$, $\ker(\varphi) \neq k$. And by **??**, $\ker(\varphi) = 0$ and hence φ is injective

Exercise 2.0.12 *Let R be a ring, $\mathfrak{p}$ a prime, $\mathcal{X}$ a set of variables. Let $\mathfrak{p}[\mathcal{X}]$ denote the set of polynomials with coefficients in $\mathfrak{p}$. Prove*

1. $\mathfrak{p}R[\mathcal{X}]$ *and* $\mathfrak{p}[\mathcal{X}]$ *and* $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ *are primes of* $R[\mathcal{X}]$*, which contract*

to $\mathfrak{p}$

2. *Assume* $\mathfrak{p}$ *is maximal. Then* $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ *is maximal*

1. $R/\mathfrak{p}$ is a domain. $\mathfrak{p}R[\mathcal{X}] = \mathfrak{p}[\mathcal{X}]$ by **??**.

   $(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle/\mathfrak{p}R[\mathcal{X}])$ is equal to $\langle\mathcal{X}\rangle \subset (R/\mathfrak{p})[\mathcal{X}]$. $(R/\mathfrak{p})\langle\mathcal{X}\rangle/\langle\mathcal{X}\rangle$ is equal to $R/\mathfrak{p}$. Hence $R[X]/(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle) = (R[x]/\mathfrak{p}R[X])/((\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle)/\mathfrak{p}R[X]) = R/\mathfrak{p}$

   Since the canonical map $R/\mathfrak{p} \to R[\mathcal{X}]/(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle)$ is bijective, it's injective.

2. $R/\mathfrak{p} \simeq R[\mathcal{X}]/(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle)$

Exercise 2.0.13 *Let R be a ring, X a variable, $H \in P := R[X]$ and $a \in R$. Given $n \geq 1$, show $(X-a)^n$ and H are coprime iff $H(a)$ is a unit.*

$(X-a)^n$ and H are coprime iff $X-a$ and H are coprime. $R[x]/\langle X-a\rangle = \langle H\rangle/\langle X-a\rangle$, which implies the residue of H modulo $X-a$ is a unit. Hence $H(a)$ is a unit.

Exercise 2.0.14 *Let R be a ring, X a variable, $F \in P := R[X]$, and $a \in R$. Set $F' := \partial F/\partial X$. Show the following statements are equivalent*

1. *a is a supersimple root of F*
2. *a is a root of F, and $X-a$ and F' are coprime*

3. $F = (X - a)G$ for some G in P coprime to $X - a$

Show that if (3) holds, then G is unique

Exercise 2.0.15 *Let R be a ring, $\mathfrak{p}$ a prime; $\mathcal{X}$ a set of variables; $F, G \in R[\mathcal{X}]$. Let $c(F)$, $c(G)$, $c(FG)$ be the ideals of R generated by the coefficients of F, G, FG*

1. *Assume $\mathfrak{p}$ doesn't contain either $c(F)$ or $c(G)$. Show $\mathfrak{p}$ doesn't contain $c(FG)$*

2. *Assume $c(F) = R$ and $c(G) = R$. Show $c(FG) = R$*

1. Denote the residues of F, G, FG in $(R/\mathfrak{p})[\mathcal{X}]$ by F, G and FG. Since

$\mathfrak{p} \not\supset c(F), c(G)$, $F, G \neq 0$. Since $R/\mathfrak{p}$ is a domain, so is $(R/\mathfrak{p})[\mathcal{X}]$ and we have $FG \neq 0$. Note that $FG = FG$, we have $FG \neq 0$.

2. Assume $c(F) = c(G) = R$, since $\mathfrak{p} \not\supset c(F), c(G)$ we have $\mathfrak{p} \not\supset c(FG)$ for any prime ideals $\mathfrak{p}$. Hence $c(FG) = R$.

   If $c(FG) = R$, $c(FG) \subset c(F)$

Exercise 2.0.16 *Let B be a Boolean ring. Show that every prime $\mathfrak{p}$ is maximal, and that $B/\mathfrak{p} = \mathbb{F}_2$*

$x(x-1) = 0$ in $B/\mathfrak{p}$. Since $B/\mathfrak{p}$ is a domain, $x = 0$ or $x = 1$.

Exercise 2.0.17 *Let R be a ring. Assume that, given any $x \in R$, there is* *an $n \geq 2$ with $x^n = x$. Show that every prime $\mathfrak{p}$ is maximal*

Same. Every element has an inverse

Exercise 2.0.18 *Prove the following statements or give a counterexample*

1. *The complement of a multiplicative subset is a prime ideal*

2. *Given two prime ideals, their intersection is prime*

3. *Given two prime ideals, their sum is prime*

4. *Given a ring map $\varphi : R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R*

5. *An ideal $\mathfrak{m}' \subset R/\mathfrak{a}$ is maximal iff $\kappa^{-1}\mathfrak{m}' \subset R$ is maximal in* **??**

1. 0 can be belongs to the multiplicative subset

2. False. In $\mathbb{Z}$, $\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle$

3. False. In $\mathbb{Z}$, $\langle 2\rangle + \langle 3\rangle = \mathbb{Z}$

4. False. Consider $\varphi : \mathbb{Z} \to \mathbb{Q}$. $\varphi^{-1}(\langle 0\rangle) = \langle 0\rangle$

5.

3 Radicals

Definition 3.1 () *Let R be a ring. Its (Jacobson)* ***radical*** (R) *is defined to be the intersection of all its maximal ideals*

Proposition 3.2 () *Let R be a ring, $\mathfrak{a}$ an ideal, $x \in R, u \in R^{\times}$. Then*

$x \in (R)$ iff $u - xy \in R^\times$ for all $x \in R$. In particular, the sum of an element of (R) and a unit is a unit, and $\mathfrak{a} \subset (R)$ if $1 - \mathfrak{a} \in R^\times$

Assume $x \in (R)$. Given a maximal ideal $\mathfrak{m}$, suppose $u - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$ too, also $u \in \mathfrak{m}$, a contradiction. Thus $u - xy$ is a unit by **??**. In particular, tkaing $y := -1$ yields $u + x \in R^\times$

Conversely, assume $x \notin (R)$. Then there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. So $\langle x \rangle + \mathfrak{m} = R$. Hence there exists $y \in R$ and $m \in \mathfrak{m}$ s.t. $xy + m = u$. Then $u - xy = m \in \mathfrak{m}$. A contradiction

In particular, given $y \in R$, set $a := u^{-1}xy$. Then $u - xy = u(1-a) \in R^\times$ if $1 - a \in R^\times$

Corollary 3.3 () *Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa : R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset (R)$. Then (κ) is injective*

Given $e, e' \in (R)$ with $\kappa(e) = \kappa(e')$, set $x := e - e'$. Then

$$x^3 = e - e' = x$$

Hence $x(1 - x^2) = 0$. But $\kappa(x) = 0$; so $x \in \mathfrak{a}$. But $\mathfrak{a} \subset (R)$. Hence $1 - x^2$ is a unit by **??**. Thus $x = 0$. Thus (κ) is injective

Definition 3.4 () *A ring is called* ***local*** *if it has exactly one maximal ideal, and* ***semilocal*** *if it has at least one and at most finitely many*

By the ***residue field*** *of a local ring A, we mean the field $A/\mathfrak{m}$ where $\mathfrak{m}$*

is the maximal ideal of A

Lemma 3.5 (Nonunit Criterion) *Let A be a ring, $\mathfrak{n}$ the set of nonunits.*

Then A is local iff $\mathfrak{n}$ is an ideal; if so, then $\mathfrak{n}$ is the maximal ideal

Assume A is local with maximal ideal $\mathfrak{m}$. Then $A - \mathfrak{n} = A - \mathfrak{m}$ by **??**.

Thus $\mathfrak{n}$ is an ideal

Example 3.1 () *The product ring $R' \times R''$ is not local by* **??** *if both R' and R'' are nonzero. $(1, 0)$ and $(0, 1)$ are nonunits, but their sum is a unit.*

Example 3.2 () *Let R be a ring. A **formal power series** in the n variables $X_1, \ldots, X_n$ is a formal* infinite *sum of the form $\sum a_{(i)} X_1^{i_1} \ldots X_n^{i_n}$ where*

$a_{(i)} \in R$ and where $(i) := (i_1, \dots, i_n)$ with each $i_j \geq 0$. The term $a_{(0)}$ where $(0) := (0, \dots, 0)$ is called the ***constant term****. Addition and multiplication are performed as for polynomials; with these operations, these series form a ring $R[[X_1, \dots, X_n]]$*

Set $P := R[[X_1, \dots, X_n]]$ and $\mathfrak{a} := \langle X_1, \dots, X_n \rangle$. Then $\sum a_{(i)} X_1^{i_1} \dots X_n^{i_n} \mapsto a_{(0)}$ is a canonical surjective ring map $P \to R$ with kernel $\mathfrak{a}$; hence $P/\mathfrak{a} = R$

Given an ideal $\mathfrak{m} \subset R$, set $\mathfrak{n} := \mathfrak{a} + \mathfrak{m}P$. Then **??** *yields $P/\mathfrak{n} = R/\mathfrak{m}$*

A power series F is a unit iff its constant term is a unit. If $a_{(0)}$ is a unit, then $F = a_{(0)}(1 - G)$ with $G \in \mathfrak{a}$. Set $F' := a_{(0)}^{-1}(1 + G + G^2 + \dots)$;

Suppose R is a local ring with maximal ideal $\mathfrak{m}$. Given a power series

$F \notin \mathfrak{n}$, *its constant term lies outside* $\mathfrak{m}$, *so is a unit. So* F *is itself a unit.*

Hence the nonunits constitutes $\mathfrak{n}$. *Thus* P *is local.*

Example 3.3 () *Let* k *be a ring, and* $A := k[[X]]$ *the formal power series ring in one variables. A* ***formal Laurent series*** *is a formal sum of the form* $\sum_{i=-m}^{\infty} a_i X^i$ *with* $a_i \in k$ *and* $m \in \mathbb{Z}$. *Plainly, these seires form a ring* $k\{\{X\}\}$. *Set* $K := k\{\{X\}\}$

Set $F := \sum_{i=-m}^{\infty} a_i X^i$. *If* $a_{-m} \in k^{\times}$, *then* $F \in K^{\times}$; *indeed,* $F = a_{-m}X^{-m}(1-G)$ *where* $G \in A$ *and*

Assume k *is a field. If* $F \neq 0$, *then* $F = X^{-m}H$ *with* $H := a_{-m}(1-G) \in A^{\times}$. *Let* $\mathfrak{a} \subset A$ *be a nonzero ideal. Suppose* $F \in \mathfrak{a}$. *Then* $X^{-m} \in \mathfrak{a}$. *Let* n

be the smallest integer s.t. $X^n \in \mathfrak{a}$. *Then* $-m \geq n$. *Set* $E := X^{-m-n}H$.

Then $E \in A$ *and* $F = X^n E$. *Hence* $\mathfrak{a} = \langle X^n \rangle$. *Thus* A ***is a*** *PID*

Further, K *is a field. In fact,* $K = (A)$.

Let $A[Y]$ *be the polynomial ring in one variable, and* $\iota : A \hookrightarrow K$ *the inclusion. Define* $\varphi : A[Y] \to K$ *by* $\varphi|A = \iota$ *and* $\varphi(Y) = X^{-1}$. *Then* φ *is surjective. Set* $\mathfrak{m} := \ker(\varphi)$. *Then* $\mathfrak{m}$ *is maximal. So by* **??** $\mathfrak{m}$ *has the form* $\langle F \rangle$ *with* F *irreducible, or the form* $\langle p, G \rangle$ *with* $p \in A$ *irreducible and* $G \in A[Y]$. *But* $\mathfrak{m} \cap A = \langle 0 \rangle$ *as* ι *is injective. So* $\mathfrak{m} = \langle F \rangle$. *But* $XY - 1$ *belongs to* $\mathfrak{m}$, *and is clearly irreducible; hence* $XY - 1 = FH$ *with* H *a unit. Thus* $\langle XY - 1 \rangle$ *is maximal*

In addition, $\langle X, Y\rangle$ is maximal. Indeed, $A[Y]/\langle X, Y\rangle = A/\langle X\rangle = k$. Howevery ,$\langle X, Y\rangle$ is not principal, as no nonunit of $A[Y]$ divides both X and Y. Thus $A[Y]$ has both principal and nonprincipal maximal ideals, two types allows by **??**

Proposition 3.6 () *Let R be a ring, S a multiplicative subset, and $\mathfrak{a}$ an ideal with $\mathfrak{a} \cap S = \emptyset$. Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \cap S = \emptyset\}$. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$, and every such $\mathfrak{p}$ is prime*

Take $x, y \in R - \mathfrak{p}$. Then $\mathfrak{p} + \langle x\rangle$ and $\mathfrak{p} + \langle y\rangle$ are strictly larger than $\mathfrak{p}$. So there are $p, q \in \mathfrak{p}$ and $a, b \in R$ with $p + ax, q + by \in S$. Hence

$pq + pby + qax + abxy \in S$. But $pq + pby + qax \in \mathfrak{p}$, so $xy \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is prime

Exercise 3.0.1 *Let $\varphi : R \to R'$ be a ring map, $\mathfrak{p}$ an ideal of R. Show*

1. *there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ iff $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$*

2. *if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there is a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$*

Saturated multiplicative subsets

Let R be a ring, and S a multiplicative subset. We say S is **saturated** if given $x, y \in R$ with $xy \in S$, necessarily $x, y \in S$

Lemma 3.7 (Prime Avoidance) *Let R be a ring, $\mathfrak{a}$ a subset of R that is* *stable under addition and multiplication, and* $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ *ideals s.t.* $\mathfrak{p}_3, \dots, \mathfrak{p}_n$ *are prime. If* $\mathfrak{a} \not\subset \mathfrak{p}_j$ *for all* j*, then there is an* $x \in \mathfrak{a}$ *s.t.* $x \notin \mathfrak{p}_j$ *for all* j*; or equivalently, if* $\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$*, then* $\mathfrak{a} \subset \mathfrak{p}_i$ *for some* i

Assume there is an $x_i \in \mathfrak{a}$ s.t. $x_i \notin \mathfrak{p}_j$ for all $i \neq j$and $x_i \in \mathfrak{p}_i$ for every i. If $n = 2$ then clearly $x_1 + x_2 \notin \mathfrak{p}_j$ for $j = 1, 2$. If $n \geq 3$, then $(x_1 \dots x_{n-1}) + x_n \notin \mathfrak{p}_j$ for all j as, if $j = n$, then $x_n \in \mathfrak{p}_n$ and $\mathfrak{p}_n$ is prime.

Other radicals

Let R be a ring, $\mathfrak{a}$ a subset. Its **radical** $\sqrt{\mathfrak{a}}$ is the set

$$\sqrt{\mathfrak{a}} := \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n \geq 1\}$$

If $\mathfrak{a}$ is an ideal and $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then $\mathfrak{a}$ is said to be **radical**. For example, suppose $\mathfrak{a} = \bigcap \mathfrak{p}_\lambda$ with all $\mathfrak{p}_\lambda$ prime. If $x^n \in \mathfrak{a}$ for some $n \geq 1$, then $x \in \mathfrak{p}_\lambda$. Thus $\mathfrak{a}$ is radical. Hence two radicals coincide

We call $\sqrt{\langle 0 \rangle}$ the **nilradical**, and sometimes denote it by (R). We call an element $x \in R$ **nilpotent** if x belongs to $\sqrt{\langle 0 \rangle}$. We call an ideal $\mathfrak{a}$ **nilpotent** if $\mathfrak{a}^n = 0$ for some $n \geq 1$

$\langle 0 \rangle \subset (R)$. So $\sqrt{\langle 0 \rangle} \subset \sqrt{(R)}$. Thus

$$(R) \subset (R)$$

We call R **reduced** if $(R) = \langle 0 \rangle$

Theorem 3.8 (Scheinnullstellensatz) *Let R be a ring, $\mathfrak{a}$ an ideal. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$$

where $\mathfrak{p}$ runs through all the prime ideals containing $\mathfrak{a}$. (By convention, the empty intersection is equal to R)

Take $x \notin \sqrt{\mathfrak{a}}$. Set $S := \{1, x, x^2, \dots\}$. Then S is multiplicative, and $\mathfrak{a} \cap S = \emptyset$. By **??** there is a $\mathfrak{p} \supset \mathfrak{a}$, but $x \notin \mathfrak{p}$, but $x \notin \mathfrak{p}$. So $x \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} \supset \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

Proposition 3.9 () *Let R be a ring, $\mathfrak{a}$ an ideal. Then $\sqrt{\mathfrak{a}}$ is an ideal*

Assume $x^n, y^m \in \mathfrak{a}$. Then

$$(x+y)^{m+n-1} = \sum_{i+j=m+n-1} \binom{n+m-1}{j} x^i y^j$$

Thus $x+y \in \mathfrak{a}$

Alternatively by **??**

Exercise 3.0.2 *Use Zorn's lemma to prove that any prime ideal* $\mathfrak{p}$ *contains a prime ideal* $\mathfrak{q}$ *that is minimal containing any given subset* $\mathfrak{s} \subset \mathfrak{p}$

Minimal primes

Let R be a ring, $\mathfrak{a}$ an ideal, $\mathfrak{p}$ a prime. We call $\mathfrak{p}$ a **minimal prime** of $\mathfrak{a}$, or over $\mathfrak{a}$, if $\mathfrak{p}$ is minimal in the set of primes containing $\mathfrak{a}$. We call $\mathfrak{p}$ a **minimal prime** of R if $\mathfrak{p}$ is a minimal prime of $\langle 0 \rangle$

Owing to **??**, every prime of R containing $\mathfrak{a}$ contains a minimal prime of $\mathfrak{a}$. So owing to the Scheinnullstellensatz **??**, the radical $\sqrt{\mathfrak{a}}$ is the intersection of all the minimal primes of $\mathfrak{a}$.

Proposition 3.10 () *A ring R is reduced and has only one minimal prime if and only if R is a domain*

?? implies $\langle 0\rangle = \mathfrak{q}$

Exercise 3.0.3 *Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $R[[X]]$ the formal power series ring, $\mathfrak{M} \subset R[[X]]$ an ideal, $F := \sum a_n X_n \in R[[X]]$. Set $\mathfrak{m} := \mathfrak{M} \cap R$ and $\mathfrak{A} := \{\sum b_n X^n \mid b_n \in \mathfrak{a}\}$. Prove the following statements:*

1. *If F is a nilpotent, then a_n is nilpotent for all n. The converse is false*

2. *$F \in (R[[X]])$ iff $a_0 \in (R)$*

3. *Assume $X \in \mathfrak{M}$. Then X and $\mathfrak{m}$ generate $\mathfrak{M}$*

4. *Assume $\mathfrak{M}$ is maximal. Then $X \in \mathfrak{M}$ and $\mathfrak{m}$ is maximal*

5. *If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}R[[X]] = \mathfrak{A}$. However, there's an example of an R with a prime ideal $\mathfrak{a}$ s.t. $\mathfrak{a}R[[X]] \neq \mathfrak{A}$*

1. Assume F and a_i for $i < n$ nilpotent. Set $G := \sum_{i \geq n} a_i X^i$. Then $G = F - \sum_{i<n} a_i X^i$. So G is nilpotent by **??**; say $G^m = 0$ for some $m \geq 1$. Then $a_n^m = 0$

Set $P := \mathbb{Z}[X_2, X_3, \ldots]$. Set $R := P/\langle X_2^2, X_3^3, \ldots\rangle$. Let a_n be the residue of X_n. Then $a_n^n = 0$, but $\sum a_n X^n$ is not nilpotent.

2. By **??**, suppose $G = \sum b_i X^i$

$$F \in (R[[X]]) \iff 1 + FG \in R[[X]]^\times \iff 1 + a_0 b_0 \in R^\times \iff a_0 \in (R)$$

5. Take $R := \mathbb{Z}[a_1, a_2, \ldots]$ and $\mathfrak{a} := \langle a_1, \ldots\rangle$. Then $R/\mathfrak{a} = \mathbb{Z}$ and $\mathfrak{a}$ is prime.

   Given $G \in \mathfrak{a}R[[X]]$, say $G = \sum_{i=1}^m b_i G_i$ with $b_i \in \mathfrak{a}$ and $G_i = \sum_{n\geq 0} b_{in} X^n$ and $F \neq G$ for any m

Example 3.4 () *Let R be a ring, $R[[X]]$ the formal power series ring. Then* *every prime $\mathfrak{p}$ of R is the contraction of a prime of $R[[X]]$. Indeed $\mathfrak{p}R[[X]] \cap R = \mathfrak{p}$. So by* **??** *there is a prime $\mathfrak{q}$ of $R[[X]]$ with $\mathfrak{q} \cap R = \mathfrak{p}$. In fact ,a specific choice for $\mathfrak{q}$ is the set of series $\sum a_n X^n$ with $a_n \in \mathfrak{q}$. Indeed, the canonical map $R \to R/\mathfrak{p}$ induces a surjection $R[[X]] \to (R/\mathfrak{p})[[X]]$ with kernel $\mathfrak{q}$; so $R[[X]]/\mathfrak{q} = (R/\mathfrak{p})[[X]]$. But* **??** *shows $\mathfrak{q}$ may not be equal to*

$\mathfrak{p}R[[X]]$

Exercise

Exercise 3.0.4 *Let R be a ring, $\mathfrak{a} \subset (R)$ an ideal, $w \in R$ and $w' \in R/\mathfrak{a}$ its residue. Prove that $w \in R^\times$ iff $w' \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset (R)$?*

Assume $\mathfrak{a} \subset (R)$. $\mathfrak{m} \mapsto \mathfrak{m}/\mathfrak{a}$ is a bijection for maximal ideal $\mathfrak{m}$. So w

belongs to a maximal ideal of R iff w' belongs to one of $R/\mathfrak{a}$

Assume $\mathfrak{a} \not\subset (R)$, then there is a maximal ideal $\mathfrak{m}$ s.t. $\mathfrak{a} \not\subset \mathfrak{m}$. So $\mathfrak{a} + \mathfrak{m} = R$. So there are $a \in \mathfrak{a}$ and $v \in \mathfrak{m}$ s.t. $a + v = w$. Then $v \notin R^\times$ but the residue of v is w', even if $w' \in (R/\mathfrak{a})^\times$. For example, take $R := \mathbb{Z}$ and $\mathfrak{a} = \langle 2 \rangle$ and $w := 3$. Then $w \notin R^\times$ but the residue of w is $1 \in (R/\mathfrak{a})^\times$

Exercise 3.0.5 *Let A be a local ring, e an idempotent. Show $e = 1$ or $e = 0$*

$1 - e + e = 1$. Since $1 \notin \mathfrak{m}$, at least one of $1 - e$ and e doesn't belong to $\mathfrak{m}$

Exercise 3.0.6 *Let A be a ring, $\mathfrak{m}$ a maximal ideal s.t. $1 + m$ is a unit* *for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?*

Let $y \in A - \mathfrak{m}$. Then $\langle y \rangle + \mathfrak{m} = A$ and there is a $x \in A$ s.t. $xy + m = 1$. Hence xy is a unit and $\langle xy \rangle = \langle y \rangle$. y is a unit.

Exercise 3.0.7 *Let R be a ring, and S a subset. Show that S is saturated multiplicative iff $R - S$ is a union of primes.*

Assume S is saturated multiplicative. Take $x \in R - S$. Then $xy \notin S$ for all $y \in R$; in other words, $\langle x \rangle \cap S = \emptyset$. Then **??** gives a prime $\mathfrak{p} \supset \langle x \rangle$ with $\mathfrak{p} \cap S = \emptyset$. Thus $R - S$ is a union of primes.

Exercise 3.0.8 *Let R be a ring, and S a multiplicative subset. Define its* ***saturation*** *to be the subset*

$$S := \{x \in R \mid \textit{there is } y \in R \textit{ with } xy \in S\}$$

1. *Show that $S \supset S$ and that S is saturated multiplicative and that any saturated multiplicative subset T containing S also contains S*

2. *Set $U := \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$. Show that $R - S = U$*

3. *Let $\mathfrak{a}$ an ideal; assume $S = 1 + \mathfrak{a}$; set $W := \bigcup_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Show $R - S = W$*

4. *Given $f, g \in R$, show that $S_f \subset S_g$ iff $\sqrt{\langle f \rangle} \supset \sqrt{\langle g \rangle}$, where $S_f = \{f^n \mid n \geq 0\}$*

3. First take a prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $1 \notin \mathfrak{p} + \mathfrak{a}$; else, $1 = p + a$ and $p = 1 - a \in \mathfrak{p} \cap S$. So $\mathfrak{p} + \mathfrak{a}$ lies in a maximal ideal $\mathfrak{m}$. Then $\mathfrak{a} \subset \mathfrak{m}$; so $\mathfrak{m} \subset W$. But also $\mathfrak{p} \subset W$. So $U \subset W$

   Conversely, take $\mathfrak{p} \supset \mathfrak{a}$. Then $1 + \mathfrak{p} \supset 1 + \mathfrak{a} = S$. But $\mathfrak{p} \cap (1 + \mathfrak{p}) = \emptyset$. So $\mathfrak{p} \cap S = \emptyset$. Thus $U \subset W$. Thus $U = W$. Thus 2 implies (3)

4. $S_f \subset S_g$ iff $f \in S_g$ iff $hf = g^n$ iff $g \in \sqrt{\langle f \rangle}$ iff $\sqrt{\langle g \rangle} \subset \sqrt{\langle f \rangle}$

Exercise 3.0.9 *Let R be a nonzero ring, S a subset. Show S is maximal in the $\mathfrak{S}$ of multiplicative subsets T of R with $0 \notin T$ iff $R - S$ is a minimal prime*

First assume S is maximal. Then $S = S$. So $R - S$ is a union of primes $\mathfrak{p}$. Fix a $\mathfrak{p}$. Then **??** yields in $\mathfrak{p}$ a minimal prime ideal $\mathfrak{q}$. Then $S \subset R - \mathfrak{q}$. But $R - \mathfrak{q} \in \mathfrak{S}$. $S = R - \mathfrak{q}$

If $R - S$ is a minimal prime. Then $S \in \mathfrak{S}$. Given $T \in \mathfrak{S}$ with $S \subset T$, note $R - T = \bigcup \mathfrak{p}$ with $\mathfrak{p}$ prime. Fix a $\mathfrak{p}$, then $S \subset T \subset T$. So $\mathfrak{q} \supset \mathfrak{p}$. But $\mathfrak{q}$ is minimal and hence $\mathfrak{q} = \mathfrak{p}$. Hence $\mathfrak{q} = R - T$. So $S = T$

Exercise 3.0.10 *Let k be a field, X_λ for $\lambda \in \Lambda$ variables, and Λ_π for $\pi \in \Pi$ disjoint subsets of Λ. Set $P := k[\{X_\lambda\}_{\lambda\in\Lambda}]$ and $\mathfrak{p}_\pi := \langle\{X_\lambda\}_{\lambda\in\Lambda_\pi}\rangle$for all $\pi \in \Pi$. Let $F, G \in P$ be nonzero, and $\mathfrak{a} \subset P$ a nonzero ideal. Set $U := \bigcup_{\pi\in\Pi} \mathfrak{p}_\pi$.*

Show

1. *Assume* $F \in \mathfrak{p}_\pi$ *for some* $\pi \in \Pi$, *then every monomial of* F *is in* $\mathfrak{p}_\pi$

2. *Assume there are* $\pi, \rho \in \Pi$ *s.t.* $F + G \in \mathfrak{p}_\pi$ *and* $G \in \mathfrak{p}_\rho$ *but* $\mathfrak{p}_\rho$ *contains no monomial of* F. *Then* $\mathfrak{p}_\pi$ *contains every monomial of* F *and of* G

3. *Assume* $\mathfrak{a} \subset U$. *Then* $\mathfrak{a} \subset \mathfrak{p}_\pi$ *for some* $\pi \in \Pi$

4 Modules

Modules

Let R be a ring. Recall that an R**-module** M is an abelian group, written additively, with a **scalar multiplication**, $R \times M \to M$, written $(x, m) \mapsto xm$, which is

1. **distributive**, $x(m + n) = xm + xn$ and $(x + y)m = xm + xn$

2. **associative**, $x(ym) = (xy)m$

3. **unitary**, $1 \cdot m = m$

For example, if R is a field, then an R-module is a vector space. A $\mathbb{Z}$-module is just an abelian group

A **submodule** N of M is a subgroup that is closed under multiplication.; that is, $xn \in N$ for all $x \in R$ and $n \in N$. For example, the ring R is itself an R-module, and the submodules are just the ideals. Given an ideal $\mathfrak{a}$, let $\mathfrak{a}N$ denote the smallest submodule containing all products an with $a \in \mathfrak{a}$ and $n \in N$. $\mathfrak{a}N$ is equal to the set of finite sums $\sum a_i n_i$.

Given $m \in M$, we call the set of $x \in R$ with $xm = 0$ the **annihilator** of m, and denote it (m). We call the set of $x \in R$ with $xm = 0$ for all $m \in M$ the **annihilator** of M, and denote it (M)

Homomorphisms

Let R be a ring, M and N modules. A **homomorphism**, or **module map** is a map $\alpha : M \to N$ that is R**-linear**:

$$\alpha(xm + yn) = x(\alpha m) + y(\alpha n)$$

Note that f is injective iff it has a left inverse. f is surjective iff it has a right inverse

A homomorphism α is an isomorphism iff there is a set map $\beta : N \to M$

s.t. $\beta\alpha = 1_M$ and $\alpha\beta = 1_N$, and then $\beta = \alpha^{-1}$.

The set of homomorphisms α is denoted by $\mathrm{Hom}_R(M, N)$ or simply $\mathrm{Hom}(M, N)$. It is an R-module with addition and scalar multiplication defined by

$$(\alpha + \beta)m := \alpha m + \beta m \quad \text{and} \quad (x\alpha)m := x(\alpha m) = \alpha(xm)$$

Homomorphisms $\alpha : L \to M$ and $\beta : N \to P$ induce, via composition, a map

$$\mathrm{Hom}(\alpha, \beta) : \mathrm{Hom}(M, N) \to \mathrm{Hom}(L, P)$$

When α is the identity map 1_M, we write $\mathrm{Hom}(M, \beta)$ for $\mathrm{Hom}(1_M, \beta)$

Exercise 4.0.1 *Let R be a ring, M a module. Consider the map*

$$\theta : \mathrm{Hom}(R, M) \to M \qquad \textit{defined by} \qquad \theta(\rho) := \rho(1)$$

Show that θ is an isomorphism, and describe its inverse

First, θ is R-linear. Set $H := \mathrm{Hom}(R, M)$. Define $\eta : M \to H$ by $\eta(m)(x) := xm$. It is easy to check that $\eta\theta = 1_H$ and $\theta\eta = 1_M$. Thus θ and η are inverse isomorphism

Endomorphisms

Let R be a ring, M a module. An **endomorphism** of M is a homomorphism $\alpha : M \to M$. The module of endomorphism $\mathrm{Hom}(M, M)$ is also denoted $_R(M)$. Further, $_R(M)$ is a subring of $_{\mathbb{Z}}(M)$

Given $x \in R$, let $\mu_x : M \to M$ denote the map of **multiplication** by x, defined by $\mu_x(m) := xm$. It is an endomorphism. Further, $x \mapsto \mu_x$ is a ring map

$$\mu_R : R \to_R (M) \subset_{\mathbb{Z}} (M)$$

(Thus we may view μ_R as representing R as a ring of operators on the abelian gorup). Note that $\ker(\mu_R) = (M)$

Conversely, given an abelian group N and a ring map

$$\nu : R \to_{\mathbb{Z}} (N)$$

we obtain a module structure on N by setting $xn := (\nu x)(n)$. Then $\mu_R = \nu$

We call M **faithful** if $\mu_R : R \to_R (M)$ is injective, or $(M) = 0$. For example, R is a faithful R-module for $x \cdot 1 = 0$ implies

Algebras

Fix two rings R and R'. Suppose R' is an R-algebra with structure map φ. Let M' be an R'-module. Then M' is also an R-module by **restriction on scalars**: $xm := \varphi(x)m$. In other words, the R-module structure on M' corresponds to the composition

$$R \xrightarrow{\varphi} R' \xrightarrow{\mu_{R'}}_{\mathbb{Z}} (M')$$

In particular, R' is an R-module; further, for all $x \in R$ and $y, z \in R'$

$$(xy)z = x(yz)$$

by restriction on scalars

Conversely, suppose R' is an R-module s.t. $(xy)z = x(yz)$. Then R' has an R-algebra structure that is compatible with the given R-module structure.. Indeed, define $\varphi : R \to R'$ by $\varphi(x) := x \cdot 1$. Then $\varphi(x)z = xz$ as $(x \cdot 1)z = x(1 \cdot z)$. So the composition $\mu_{R'}\varphi : R \to R' \to_{\mathbb{Z}} (R')$ is equal to μ_R. Hence φ is a ring map. Thus R' is an R-algebra, and restriction of scalars recovers its given R-module structure

Suppose that $R' = R/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Then an R-module M has a compatible R'-module structure iff $\mathfrak{a}M = 0$; if so, then the R'-structure is unique. Indeed, the ring map $\mu_R : R \to_{\mathbb{Z}} (M)$ factors through R' iff

$\mu_R(\mathfrak{a}) = 0$, so iff $\mathfrak{a}M = 0$

Again suppose R' is an arbitrary R-algebra with structure map φ. A **subalgebra** R'' of R' is a subring s.t. φ maps into R''. The subalgebra **generated** by $x_1, \ldots, x_n \in R'$ is the smallest R-subalgebra that contains them. We denote it by $R[x_1, \ldots, x_n]$.

We say R' is a **finitely generated** R**-subalgebra** or is **algrbra finite over** R if there exist $x_1, \ldots, x_n \in R'$ s.t. $R' = R[x_1, \ldots, x_n]$

Residue modules

Let R be a ring, M a module, $M' \subset M$ a submodule. Form the set of cosets

$$M/M' := \{m + M' \mid m \in M\}$$

M/M' inherits a module structure, and is called the **residue module** or **quotient of M modulo M'**. Form the **quotient map**

$$\kappa : M \to M/M' \quad \text{by} \quad \kappa(m) := m + M'$$

Clearly κ is surjective, κ is linear, and κ has kernel M'

Let $\alpha : M \to N$ be linear. Note that $\ker(\alpha') \supset M'$ iff $\alpha(M') = 0$

If $\ker(\alpha) \supset M'$, then there exists a homomorphism $\beta : M/M' \to N$ s.t.

$\beta\kappa = \alpha$

M[r,"κ"][rd,"α"]$M/M'[d$,"β"]

N

Always

$$M/\ker(\alpha)(\alpha)$$

M/M' has the following UMP: $\kappa(M') = 0$, and given $\alpha : M \to N$ s.t. $\alpha(M') = 0$, there is a unique homomorphism $\beta : M/M' \to N$ s.t. $\beta\kappa = \alpha$

Cyclic modules

Let R be a ring. A module M is said to be **cyclic** if there exists $m \in M$ s.t. $M = Rm$. If so, form $\alpha : R \to M$ by $x \mapsto xm$; then α induces an isomorphism $R/(m)M$. Note that $(m) = (M)$. Conversely, given any ideal $\mathfrak{a}$, the R-module $R/\mathfrak{a}$ is cyclic, generated by the coset of 1, and $(R/\mathfrak{a}) = \mathfrak{a}$

Noether Isomorphisms

Let R be a ring, N a module, and L and M submodules.

First, assume $L \subset M \subset N$. Form the following composition of quotient maps:

$$\alpha : N \to N/L \to (N/L)/(M/L)$$

α is surjective and $\ker(\alpha) = M$. Hence

N[r][d]N/M[d,"β”,” $\simeq$ ”′]

N/L[r](N/L)/(M/L)

Second, let $L+M$ denote the set of all sums $l+m$ with $l \in L$ and $m \in M$.

Clearly $L + M$ is a submodule of N. It is called the **sum** of L and M

Form the composition α' of the inclusion map $L \to L + M$ and the quotient map $L + M \to (L + M)/M$. Clearly α' is surjective and $\ker(\alpha') = L \cap M$. Hence

L[r][d]L/(L$\cap$$M$)[$d$,"$\beta'$"," $\simeq$ "$'$]

L+M[r](L+M)/M

Cokernels, coimages

Let R be a ring, $\alpha : M \to N$ a linear map. Associated to α are its **cokernel** and its **coimage**

$$(\alpha) := N/(\alpha) \quad \text{and} \quad (\alpha) := M/\ker(\alpha)$$

they are quotient modules, and their quotient maps are both denoted by κ.

UMP of the cokernel: $\kappa\alpha = 0$ and given a map $\beta : N \to P$ with $\beta : N \to P$ with $\beta\alpha = 0$, there is a unique map $\gamma : (\alpha) \to P$ with $\gamma\kappa = \beta$

M[r,"α"][rd]$N[d,"\beta"][r,"\kappa"](\alpha)[ld,"\gamma"]$

P

Further, $(\alpha)(\alpha)$

Free modules

Let R be a ring, Λ a set, M a module. Given elements $m_\lambda \in M$ for $\lambda \in \Lambda$, by the submodule they **generate**, we mean the smallest submodule that contains then all. Clearly, any submodule that contains them all contains any (finite) linear combination $\sum x_\lambda m_\lambda$ with $x_\lambda \in R$

m_λ are said to be **free** or **linearly independent** if whenever $\sum x_\lambda m_\lambda = 0$, also $x_\lambda = 0$ for all λ. Finally, the m_λ are said to form a **free basis** of M if they are free and generate M; if so, then we say M is **free** on the m_λ

We say M is **free** if it has a free basis. Any two free bases have the same number l of elements, and we say M is **free of rank** l

For example, form the set of **restricted vectors**

$$R^{\oplus\Lambda} := \{(x_\lambda) \mid x_\lambda \in R \text{ with } x_\lambda = 0 \text{ for almost all } \lambda\}$$

It's a module under componentwise addition and scalar multiplication. It has a **standard basis**, which consists of the vectors e_μ whose λth component is the value of the **Kronecker delta function**

If Λ has a finite number l of elements, then $R^{\oplus\Lambda}$ is often written R^l and called the **direct sum of l copies** of R

The free module $R^{\oplus\Lambda}$ has the following UMP: given a module M and elements $m_\lambda \in M$ for $\lambda \in \Lambda$, there is a unique homomorphism

$$\alpha : R^{\oplus\Lambda} \to M \text{ with } \alpha(e_\lambda) = m_\lambda \text{ for each } \lambda \in \Lambda$$

namely, $\alpha((x_\lambda)) = \alpha(\sum x_\lambda e_\lambda) = \sum x_\lambda m_\lambda$. Note the following obvious statements:

1. α is surjective iff m_λ generate M

2. α is injective iff m_λ are linearly independent

3. α is an isomorphism iff m_λ for a free basis

Thus M is free of rank l iff $M \simeq R^l$

Exercise 4.0.2 *Take $R := \mathbb{Z}$ and $M := \mathbb{Q}$. Then any two $x, y \in M$ are not free. Aso M is not finitely generated. Indeed, given any $m_1/n_1, \ldots, m_r/n_r \in M$, let d be a common multiple of $n_1, \ldots, n_r$. Then $(1/d)\mathbb{Z}$ contains every linear combination but $(1/d)\mathbb{Z} \neq \mathbb{Q}$*

Exercise 4.0.3 *Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of (R) generated by $1, x^{-1}, x^{-2}, \ldots$. Suppose that M is finitely* *generated. Prove that* $x^{-1} \in R$ *and conclude that* $M = R$

Suppose M is generated by $m_1, \ldots, m_k$. Say $m_i = \sum_{j=0}^{n_i} a_{ij} x^{-j}$ for some n_i and $a_{ij} \in R$. Set $n := \max\{n_i\}$. Then $1, x^{-1}, \ldots, x^{-n}$ generate M. So

$$x^{-n+1} = a_n x^{-n} + \cdots + a_0$$

Thus

$$x^{-1} = a_n + \cdots + a_0 x^n$$

Direct Products, Direct Sums

Let R be a ring, Γ a set, M_λ a module for $\lambda \in \Lambda$. The **direct product** of the M_λ is the set of arbitrary vectors:

$$\prod M_\lambda := \{(m_\lambda) \mid m_\lambda \in M_\lambda\}$$

The **direct sum** of the M_λ is the subset of **restricted vectors**:

$$\bigoplus M_\lambda := \{(m_\lambda) \mid m_\lambda = 0 \text{ for almost all } \lambda\} \subset \prod M_\lambda$$

The direct product comes equipped with projections

$$\pi_\kappa : \prod M_\lambda \to M_\kappa \quad \text{given by} \quad \pi_\kappa((m_\lambda)) := m_\kappa$$

$\prod M_\lambda$ has UMP: given homomorphisms $\alpha_\kappa : N \to M_\kappa$, there is a unique homomorphism $\alpha : N \to \prod M_\lambda$ satisfying $\pi_\kappa \alpha = \alpha_\kappa$ for all $\kappa \in \Lambda$; namely $\alpha(n) = (\alpha_\lambda(n))$. Often α is denoted (α_λ). In other words, the π_λ induce a bijection of sets

$$\mathrm{Hom}(N, \prod M_\lambda) \prod \mathrm{Hom}(N, M_\lambda)$$

Similarly, the direct sum comes equipped with injections

$$\iota_\kappa : M_\kappa \to \bigoplus M_\lambda \quad \text{given by} \quad \iota_\kappa(m) := (m_\lambda) \text{ where } m_\lambda := \begin{cases} m & \lambda = \kappa \\ 0 & \end{cases}$$

UMP: given homomorphisms $\beta_\kappa : M_\kappa \to N$, there is a unique homomorphism $\beta : \bigoplus M_\lambda \to N$ satisfying $\beta\iota_\kappa = \beta_\kappa$ for all $\kappa \in \Lambda$ for all $\kappa \in \Lambda$; namely, $\beta((m_\lambda)) = \sum \beta_\lambda(m_\lambda)$. Often β is denoted $\sum \beta_\lambda$; often (β_λ). In other words, the ι_κ induce this bijection of sets:

$$\operatorname{Hom}(\bigoplus M_\lambda, N) \prod \operatorname{Hom}(M_\lambda, N) \tag{4.0.1}$$

For example, if $M_\lambda = R$ for all λ, then $\bigoplus M_\lambda = R^{\oplus\Lambda}$. Further, if $N_\lambda := N$ for all λ, then $\operatorname{Hom}(R^{\oplus\Lambda}, N) = \prod N_\lambda$ by (**??**) and **??**

Exercise 4.0.4 *Let Λ be an infinite set, R_λ a ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but $\bigoplus R_\lambda$ does not (so is not a ring)*

Exercise 4.0.5 *Let L, M, N be modules. Consider a diagram*

$$L[r, "\alpha", yshift = 0.7ex]M[r, "\beta", yshift = 0.7ex][l, "\rho", yshift =$$

$$-0.7ex]N[l, "\sigma", yshift = -0.7ex]$$

where α, β, ρ and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \textit{and} \quad \alpha = \iota_L, \beta = \pi_N, \sigma = \iota_N, \rho = \pi_L$$

iff the following relations holds

$$\beta\alpha = 0, \beta\sigma = 1, \rho\sigma = 0, \rho\alpha = 1, \alpha\rho + \sigma\beta = 1$$

Consider the map $\varphi : M \to L \oplus N$ and $\theta : L \oplus N \to M$ given by $\varphi m := (\rho m, \rho m)$ and $\theta(l, n) := \alpha l + \sigma n$. They are inverse isomorphism since

$$\varphi\theta(l, n) = (\rho\alpha l + \rho\sigma n, \beta\alpha l + \beta\sigma n) = (l, n) \quad \text{and} \quad \theta\varphi m = \alpha\rho m + \sigma\beta m = m$$

Exercise 4.0.6 *Let N be a module, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove that the injections $\iota_\kappa : M_\kappa \to \bigoplus M_\lambda$ induce an injection*

$$\bigoplus \operatorname{Hom}(N, M_\lambda) \hookrightarrow \operatorname{Hom}(N, \bigoplus M_\lambda)$$

and that it is an isomorphism if N is finitely generated

For $(\beta_\kappa) \in \bigoplus \operatorname{Hom}(N, M_\lambda)$

$$\beta(n) = \begin{cases} \iota_\kappa \beta_\kappa & \text{if } \beta_\kappa \neq 0 \\ 0 & \beta_\kappa = 0 \end{cases} \in \operatorname{Hom}(N, \bigoplus M_\lambda)$$

If N is fintitely generated, suppose $a_1, \ldots, a_n$ generates N and $\beta(a_i) = b_i \in \bigoplus M_\lambda$, which means $\beta(N)$ is a finite direct subsum of $\bigoplus M_\lambda$. then we have