Abstract Algebra II

Mark

Chapter 7, recall

Ring is an **abelian** additive group with multiplication that's **associative** and **closed**, linked by **distribution**.

Division Ring: a ring with mult inverses
Zero Divisor: if there is another element so product is zero
Integral Domain: commutative ring with unit and no zero divisors.

Ideal: subring I such that ir and $ri \in I$ for all r in ring.
For I, J ideals,

$$IJ = \text{ set of finite sums of ij}$$

principle ideal: ideal generated by one element using + and *
maximal ideal: ideal not contained in any other proper ideal.
prime ideal: ab in ideal, then a or b is.

$$\boxed{P \text{ is prime} \iff R/P \text{ is an integral domain}}$$

see notes for proof.

$$\boxed{M \text{ is maximal} \iff R/M \text{ is a field}}$$

R/M is field means no ideals; by lattice iso, no ideals between R and M.

maximal ideal → prime ideal

max ideal → R/P is a field.
field is an integral domain.

Quadratic Fields and integer rings

Define a **quadratic field** as

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

for $D \in \mathbb{Q}$ and not divisible by a perfect square ('square-free').

can show this is a field using usual checks.

Inverses * involves a trick :
key: $(a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2$
If a and b are not both zero, then, $a^2 - Db^2$ can't be zero.
(this would imply $D = \frac{a}{b}^2$, a contradiction) Thus,

$$(a+b\sqrt{D})\frac{a-b\sqrt{D}}{a^2-Db^2} = 1$$

For $D=-1$, $\mathbb{Z}[D]$ is $\mathbb{Z}[i]$, the set $a+bi$ with integer coefficients, called the **Gaussian Integers**.

Define the **quadratic ring of integers**, Θ_D, in the quadratic field $\mathbb{Q}(\sqrt{D})$ as

$$\begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D = 2,3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}], & \text{if } D = 1 \bmod 4 \end{cases}$$

*note both $\mathbb{Z}[\sqrt{D}]$ and $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ are subrings of the field $\mathbb{Q}(\sqrt{D})$.

The **field norm** N is a function from $\mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ defined

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2$$

(as noted above norm is never zero if both a and b are not zero)

For the ring of integers ("quadratic integer rings"), the norm is more genrally defined as

$$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega})$$

where $\bar{\omega}$ is the Galois conjugate (-) is attached to $\sqrt{D}$.

Norm is **multiplicative**: $N(\alpha\beta) = N(\alpha)N(\beta)$.

a number in $\mathbb{Q}[\sqrt{D}]$ is an **algebraic integer** if it's the root of a monic polynomial with integer coefficients.

α is a unit implies there exists β such that $\alpha\beta = 1$.

An element α in the ring of integers is a **unit** if and only if $N(\alpha) = \pm 1$.

proof: $\rightarrow$) Suppose α is a unit. Then,

$$\alpha\beta = 1, \text{ for some } \beta \in \Theta_D$$

So, $N(\alpha\beta) = N(1) = 1$.
$\leftarrow$) $\alpha\bar{\alpha} = \pm 1$, so either $\alpha\bar{\alpha} = 1$ or $\alpha(-\bar{\alpha}) = 1$.

e.g., for $\mathbb{Z}[i]$ (aka $D = -1$), the units are $\{\pm 1, \pm i\}$ as they are the only option satisfying $a^2 + b^2 = 1$.

For rings, $A, B, AB = \{a_1b_1 + a_2b_2 + a_3b_2 + ...\}$ "finite sums of elements"

Ideal generated by a subset of R, A is denoted (A).
it's the "smallest ideal containing A"
Kernel of a ring homomorphism is set of elements mapping to 0 (additive id).

$$\boxed{\text{Kernel of ring hom is an ideal}}$$

For $s \in Kernel$, any $r \in R$, consider $\varphi(sr)$ still maps to kernel.
hence ker is ideal

Exercises

1. What are the units of $\Theta_{-3} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$?
   $\alpha = a + b\frac{1+\sqrt{-3}}{2}$ is a unit $\iff$
   N(α) $= a^2 + ab + b^2 = 1$
   TRICK: complete the square!
   $(2a+b)^2 + 3b^2 = 4$
   only options for b are $0, 1$, or -1.
   units are $\{\pm 1, \pm\frac{1}{2}, \pm\frac{\sqrt{-3}}{2}\}$.

2. Prove $\mathbb{Z}[i]$ with $N(a + bi) = a^2 + b^2$ is a Euclidean Domain.
   We need to show Division Algo works.
   For $\alpha, \beta \in \mathbb{Z}[i]$, $(\beta \neq 0)$
   $$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{a}{c^2+d^2} + \frac{bi}{c^2+d^2} = r + si \quad (r, s \in \mathbb{Q})$$
   Let p, q be the closest integers to r, s in turn. Then,
   $$N((r+si) - (p+qi)) = (r-p)^2 + (s-q)^2 \leq \frac{1}{2}$$
   Then, we define Algo as
   $$\alpha = (p+qi)\beta + R$$
   Remains to show $N(R) < N(\beta)$.
   Define some other variable $\theta = (r-p) + (s-q)i$, with $N(\theta) < \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.
   Then,
   $$N(R) = N(\theta)N(\beta) \leq \frac{1}{2}N(\beta)$$

3. Find the ideal generated by $(3-i, 2+11i)$.
   idea is to find the gcd using Euclidean Algo.
   First,
   $$\frac{2+11i}{3-i} = \frac{-1}{2} + \frac{7}{2}i.$$
   Select closests integers $p = -1, q = 3$. Then remainder R is
   $$= 2 + 11i - (-1+3i)(3-i) = 2+i.$$
   We have
   $$2 + 11i = (-1+3i)(3-i) + (2+i).$$
   Next,
   $$\frac{3-i}{2+i} = (1-i)$$
   Thus,
   $$3 - i = (1-i)(2+i) + 0.$$
   Meaning, the gcd $= 2+i$ (last nonzero remainder).
   Thus, ideal is $((2+i))$.

4. Show $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Domain.
   idea is to show it's not a PID (hence not a Euclidean Domain).
   Consider $I = (2, 1+\sqrt{-5})$.
   Suppose I is a principal ideal with generator α.
   Then $2 = k_1 * \alpha$ and $1 + \sqrt{-5} = k_2\alpha$.
   Then, $N(\alpha)$ divides 4 and divides 6 $\rightarrow N(\alpha) = 1$ or 2.
   Case 1: $N(\alpha) = 2$
   Then, $2 = a^2 + 5b^2$, which is impossible for $a, b \in \mathbb{Z}$.
   Case 2: $N(\alpha) = 1$
   ...somehow contradiction

5. What are zero divisors of $/Z$? What are units?
   no zero divisors; units are ± 1. So $\mathbb{Z}^*$ $\{\pm 1\}$

Chapter 8: Euclidean Domains

Norm

For R an integral domain, a **norm** is a function N such that
$$N : R \rightarrow \mathbb{Z}_{\geq 0} \text{ and } N(0) = 0$$

A norm is a measure of size in R.

e.g., $R = F[x]$, norm is generally the degree of the polynomial.

*possible for same integral domain to have more than one norm. Often, statements are with respect to a particular norm.

Euclean Domain

A **Euclidean Domain** is an integral domain, R, with a division algorithm such that for any two elements $a, b \in R (b \neq 0)$,
there exists $q, r \in R$ where

$$a = qb + r \text{ and } r = 0 \text{ or } N(r) < N(b)$$

q is the **quotient** and r is the **remainder**.

e.g., fields (with any norm), $\mathbb{Z}$ with $N(a) = |a|$, $F[x]$ with norm = degree of polynomial.

Every ideal in a Euclidean Domain is **principal**

proof: consider d in an ideal I, such that d has minimum norm in I. (exists by Well ordering principal)

(1): $(d) \subset I$, by closure.

(2): $I \subset (d)$, since for $a \in I$,

$$a = qd + r$$

with $N(r) < N(a)$ (impossible) or $r = 0$. Thus, $a \in (d)$.

*useful to show NOT Euclidean Domain, if some ideal is not principal.

A Euclidean Domain allows for the use of the **Euclidean Algorithm**.

If (a, b) (ideal generated by a, b) = (d), then $d = gcd(a, b)$
because $d = ax + by$ by Euclidean Algo.

Principal Ideal Domains, PIDs

A **Principal Ideal Domain** is an integral domain where every ideal is principal.

Euclidean Domain → PID
since every ideal in Euclidean Domain is principal

In a PID, irreducible → prime.

For r irreducible, wwts (r) is a prime ideal.
Suppose $(r) \subset (m)$.
Then r = am for some a, then a is a unit or m is a unit since r is irreducible. a unit $\rightarrow (r) = (m)$
m unit $\rightarrow (m) =$ entire ring.

Unique Factorization Domains, UFDs

For R an integral domain,

- $r \in R$ is **irreducible** if whenever, $r = ab$ $(a, b \in R)$, a or b is a unit. (otherwise, r is **reducible**)
- $p \in R$ $(\neq 0)$, is **prime** if (p) is a prime ideal.
  i.e., normal notion of prime $p|ab$, $p|a$ or $p|b$ (aka a or b in ideal).
- $a, b \in R$ are **associate** if $a = ub$ for some unit $u \in R$.

$$\boxed{\text{prime element} \rightarrow \text{irreducible}}$$

p, prime. If $ab = p \in (p)$, then $a \in (p)$ or $b \in (p)$.
Next, show a or b is a unit.
Note without loss of generality, $p = ab = prb \rightarrow rb = 1$, meaning b is a unit.

irreducible $\not\rightarrow$ prime: e.g., $2|(1+\sqrt{-5})(1-\sqrt{-5})$, but 2 does not divide $1+\sqrt{5}$.

$$\boxed{\text{In PID, prime element} \iff \text{irreducible}}$$

above proves $\rightarrow$).
$\leftarrow$) see previous page.

A **Unique Factorization Domain** is an integral domain in which for every $r \neq 0$ and not a unit:
(1) r can be written as a **finite product** of irreducible elements.
*not necessarily distinct.
(2) above is **unique** up to associates.
*any factorization has same number of products and elements are associates with elements of composition in (1).

easiest example is any field, since every element in a field is a unit (hence nothing to verify in order be a UFD).

examples of UFDs: $\mathbb{Z}$, $\mathbb{F}[x]$, $\mathbb{Z}[i]$.
$\mathbb{Z}[i]$ showed it's a Euclidean Domain $\rightarrow$ PID $\rightarrow$ UFD. Similar proof for $F[x]$.
$\mathbb{Z}[x]$ is a UFD, but not a PID.

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD
$6 = 2 * 3$, but also $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Each produc is made of irreducible terms.

Ascending Chain Condition (ACC), Notherian

A commutative ring with unit R is **Noetherian** if it satisfies ACC:

every increasing sequence of ideas:

$$I_1 \subset I_2 \subset ...$$

terminates, eventually.

Equivalent to say:

1. ACC
2. every nonempty collection of ideals has a maximal element
3. every ideal is finitely generated

proof
$(1 \to 2)$ Suppose A is any nonempty collection of ideals.
If no maximal ideal I_n existed in the collection, we can construct an infinite chain, hence not ACC, a contradiction.

$(2 \to 3)$ Let A be a nonempty collection of ideals with a maximal element, say I_0.
Thus, for I_i in chain:
(a) $I_0 \subset I_i$, since I_0 is maximal.
(b) $I_i \subset I_0$, since unclear $(3 \to 1)$ Suppose $I_1 \subset I_2 \subset I_3 \subset ...$ is a chain of ideals
Then, $\overset{\infty}{_i} I_i$ is an ideal, say I.
Since, every ideal is finitely generated, so is I, meaning the chain terminates.

e.g., $\mathbb{Z}[x_1, ..., x_n, ...]$ is Netherian.

$(x_1) \subset (x_1, x_2) \subset ...$ infinite.

PID is Netherian

since every ideal is generated by 1 element, by (3) above, PID is Netherian.

PID $\to$ UFD

proof:
IDEA: factor such as integers.
Suppose $r \neq 0$ in R, a PID.
Then we can factor r as $r_1 * r_2$.....
Suppose a branch of the factorization continued, then we'd have a chain:
$(r_1) \subset (r_2) \subset (r_3)$
along the branch, which contradicts ACC (since PID has ACC).
Is this product unique?

Suppose $r = p_1 p_2 .. p_n = q_1 q_2 .. q_m$.
Then, $p_1 | q_1 q_2 ... q_m$, hence, $p_1 | q_i$ for some i.
Thus, $q_i = p_1 k$, but q_i is irreducible, hence p_1, q_i are associates.
Next repeat for p_2, to show $n = m$ and all are associates.

In UFD, irreducible $\iff$ prime.

proof: $\rightarrow$) P is irreducible. If $P|ab$ with $a = p_1..p_n, b = p'_1...p'_m$, then P is associate to some p_i, hence divides a or b.
$\leftarrow$) true in general.

Field is a ED, is a PID, is a UFD, is an Integral Domain.
(nicest to less)

GCD

An **ideal is a gcd** d of a, b if
(1) If $(a) \subset (d)$ and $(b) \subset (d)$ implies $(a, b) \subset (d)$.
(2) If $(a, b) \subset (c)$, then $(d) \subset (c)$.
"gcd(a, b) is a generator for smallest principal ideal containing (a, b)"

*(2) is a bit counterintuitive, careful.

gcds exist in UFD
gcd(a, b) = min power of primes in a, b

In PID, $(a, b) = (d)$. (exists since PID is UFD).
(but no Euclidean Algo!)

*gcd is not always a linear combo if not in PID.
e.g., $\mathbb{Z}[x]$ (UFD not PID)
a = 2, b = x: gcd(2, x) = 1
but $1 \neq 2s + xt$ for any s, t.

Euclidean domain for gcd, is even better: linear combo and algo (euclidean) to find it!

Davenport-Hasse Norm

R has a **Davenport-Hasse** norm N ifj:
For $a, b \neq 0$, $a \in (b)$ or $N(as + bt) < N(b)$ for some s, t.

e.g., Euclidean Domain has a Davenport-Hasse norm, since $N(R) = N(a - qb) < N(b)$.

Arithmetic, applying gcd

Recall, for integer rings θ_D: PID $\iff$ UFD
D < 0: almost never a PID
D > 0: unknown when they're PID.

θ_D has **no unique factorization** for elements; it does have unique factorization for ideals. (every ideal can be written as a product of prime ideals)

$\boxed{\begin{array}{l} I = (a_1, ..., a_n) = r_1 a_1 + ... + r_n a_n \text{ (r in ring)} \\ \text{"linear combos of generator elements"} \end{array}}$

For $J = (b_1, ..., b_m)$.

$$IJ = ra_1 b_1 + ... + ra_1 b_m$$
$$+ra_2 b_1 + ... + r_{a2} b_m$$

e.g., $R = \mathbb{Z}[\sqrt{-5}]$, recall not PID.
$P = (2, 1 + \sqrt{-5})$ we showed was not principal, BUT
$P^2 = (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})$
$= (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5})$ by def of $P * P$ as linear combos
$= (4, 2, 2\sqrt{-5}) = (2)$.

Irreducibles in Integer Rings

For π in integer ring, θ_D,

$$\boxed{\text{If } N(\pi) = p \text{ (for } p \text{ prime in } \mathbb{Z}\text{), } \pi \text{ is } \textbf{irreducible}}$$

Suppose $N(\pi) = p$.
Then for $\pi = ab$, $p = N(a)N(b)$
$\rightarrow N(a) = 1$ or $N(b) = 1$, meaning a or b is a unit.

What are the irreducible elements in $\mathbb{Z}[i]$?
look at $p \in \mathbb{Z}$ and see how they factor in $\mathbb{Z}[i]$. read and take notes on end of section 8.3

$$\boxed{p \text{ factors in } \mathbb{Z}[i] \text{ into two irreducibles} \iff p = a^2 + b^2 \text{ for } a, b \in \mathbb{Z}}$$

idea is to think about norm of elements factoring p

Use tool from Number Theory:

$$\text{prime } p \in \mathbb{Z} \text{ divides } n^2 + 1 \iff p \cong 1 mod 4 \text{ or } p = 2$$

look at elements of order 4 in $\mathbb{Z}/p\mathbb{Z}$ look at again

Fermat's Sum of Squares

$$\boxed{p = a^2 + b^2 \iff p \cong 1 mod 4 \text{ or } p = 2}$$

Furthermore, the sum of squares representation is **unique** up to sign changes.

What are irreducibles in $\mathbb{Z}[i]$?

$1+i$, $p \cong 3 mod 4$ for prime in $\mathbb{Z}$, and
$a \pm bi$ which form $p = a^2 + b^2$ for $p \cong 1 mod 4$ (p prime) reread 8.3 end to understand proof

For $n = 2^k p_1^{a_1} p_2^{a_2} ... p_r^{a_r} q_1^{b_1} ... q_s^{b_s}$,

$$\boxed{\text{if p, q are distinct primes with } p_i \cong 1 \mod 4 \text{ and } q_i \cong 4 \mod 4\text{, then } n \text{ can be written as the sum of squares}}$$

*the number of representations of n as a sum of squares is
$4(a_1+1)(a_2+1)...(a_r+1)$. proof at end of 8.3

Exercises

1. Show $\mathbb{Z}[2i]$ is not a UFD
   find an element written as product of different irreducibles.
   $4 = 2 * 2 = 2i(-2i)$, all irreducible.
2. Is p $= (2, 1+\sqrt{-5})$ a prime ideal in $\mathbb{Z}[\sqrt{-5}]$?
   consider quotient $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}$.
   Is it an integral domain?
   note in quotient, $\overline{1+\sqrt{-5}} = \bar{0} \to \overline{\sqrt{-5}} = \overline{-1}$.
   Thus, $\overline{a+b\sqrt{-5}} = \overline{a-b}$.
   So, $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}/(2)$ (by previous work). Thus, it is an integral domain.

Chapter 9: Polynomial Rings

Constructing $\mathbb{Q}$ from $\mathbb{Z}$
set: (a, b) with $a, b \in \mathbb{Z}$
equivalence: $(a, b) \equiv (c, d) \iff ad - bc = 0$ can confirm operations are well-defined as expected (based on representatives from equivalence class)

R UFD

Gauss's Lemma

$$\boxed{\text{p(x) reducible in } F[x] \implies \text{p(x) reducible in } R[x]}$$

proof idea: use unique factorization in UFD

$$p(x) \text{ is irreducible in } R[x] \iff \text{it is irreducible in } F[x]$$

Part by Gauss's other by looking at gcd of coefficients of $p(x)$.

$$R \text{ is UFD} \iff R[x] \text{ is UFD}$$

proof from notes and in section 8.2

Rational Roots Test

If polynomial with integer coefficients has a **rational root** r/s, r divides constant term and s divides leading coefficient.
think about factoring

Smaller Fields

For I ideal,

$$\boxed{\text{If the image of } p(x) \text{ is } \textbf{irreducible} \text{ in } R/I[x]\text{, then it's } \textbf{irreducible} \text{ in } R[x]}$$

*careful: reducible in modulo doesn't imply reducible in ring.

Take away: $\boxed{p(x) \text{ is irreducible in say } \mathbb{Z}/p\mathbb{Z} \implies p(x) \text{ irred in } Z[x]}$

content of $p(x) \in R[x]$, UFD = gcd of coefficients, "ideal generated by coef"

Roots of Polynomials

degree n polynomial has **n roots** in F, a field.
*not true in rings: $x^2 - 1$ in $\mathbb{Z}/8\mathbb{Z}[x]$ has only 4 roots.

Eisentein's Irreducibility Criterion

$p(x)$ is **irreducible** in $\mathbb{Z}[x]$ if
there is p, **prime dividing** all coefficients, but p^2 **doesn't divide** constant

More generally true for **integral domain** R: $p(x)$ irreducible in $R[x]$ if coefficients are elements of prime ideal P, but constant is not element of P^2.

$$\boxed{\text{Tip: } f(x) \text{ is irreducible} \iff \text{f(x+1) is}}$$

Exercises

1. Show $x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$.
   Since any rational root has to divide 1, the only candidates for roots are ± 1.
   Neither is a root.
   So, polynomial is irreducible.

2. Is $x^3 + 5x - 17$ irreducible in $\mathbb{Z}[x]$?
   check mod 2: $x^3 + x + 1$, which has no roots so irreducible!

Chapter 10: Modules

Linear Algebra Revisted

Linear Transformation is a homomorphism $\varphi : V \to W$ both vector spaces:
1) $\varphi(V + W) = \varphi(V) + \varphi(W)$
2) $\varphi(\alpha V) = \alpha\varphi(V)$

$T : V \to W$ a linear transformation can be **written as a matrix**:
M_b^ϵ where b is a basis of V and ϵ is a basis of W.

*note T depends on the basis chosen for V and W.

Big Theorem: every vector space has a basis.
(same number of elements as dimensionality of vector space)

Ker(T) = null space

Module

An R-module M is an **abelian group** with R, a ring, acting on M by:
1) $r(m + n) = rm + rn$
2) $(r + s)m = rm + sm$
3) $(rs)m = r(sm)$

*if R has unit, then additional requirement: 1m = m.
Examples

- F-module is a vector space over F
- $\mathbb{Z}$-module is an abelian group
- $F[x]$-module is a vectorspace V over field F with a linear transformation

Quotient Modules

For any N, M R-modules with $N \subseteq M$,

$$M/N \text{ is a quotient}$$

"all quotients are submodules"
why? 1. $N \trianglelefteq M$ since N is abelian. so "+" makes sense
2. $r(m + N) = rm + N$ just need to check it's well-defined.

Generators

Idea in general "blah" **generated by** $m_1, m_2, ..., m_n$ means the **smallest "blah" stucture** containing all m_i.

Sub-module generated by $m_1, m_2, ..., m_n \in M$ is

$$Rm_1, +... + Rm_n$$

since closure is over addition and scalar mult, both captured above by linear combo
cyclic R-module if generated by a single element.

submodule

N is a sub-module of a module M if for $n_1, n_2 \in N$,

1. $n_1 + n_2 \in N$ "closure +"
2. $rm_1 \in N$ "scalar closure"

Homomorphisms

$\varphi : M \to N$
R-module homomorphism φ is what you'd expect:
$\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(rx) = r\varphi(x)$.
Ker(φ) and Image(φ) are both submodules (in M, N in turn)

Isomorphism Theorems

- $M/\text{ Ker}\varphi \cong \text{Image}(\varphi)$
- $A + B/B \cong A/A \cap B$
- $(M/N)/(M'/N) \cong M/M' \quad$ for $N \subseteq M' \subseteq M$

and lattice bien sur.

Cyclic Modules

a **module** M is **cyclic** means there exists $m \in M$ such that $R * m = M$.

an element a of M is **torsion-free** if $ra \neq 0$ for any $r \in R$.
(a is **torsion** element if there is some r such that $ra = 0$)

*torsion module implies every element is a torsion element.

Natural Map for Cyclic Modules (over PIDs)

$\varphi : R \to M$ by $r \to rm$ where m is generator.

Ker(φ) = left ideal in R, call it I. Then,

$$R/I \cong M$$

by first iso theorem. idea: $M = R * m$, so it's isomorphic to left cosets of R: $R/(r)$.
*idea: nicer ring, yields nicer r-module M.
"annihilator" of M in $R = \{r \in R : rm = 0 \text{ for all } m\}$

Properties of Determinants

- $det(I_n) = 1$
- $det(A^T) = det(A)$
- $det(A^{-1}) = det(A)^{-1}$ (i.e., 1/ det(A))
- $det(AB) = det(A)det(B)$ (= det(BA)) "commutative"
- $det(cA) = c^n det(A)$ for c a constant
- for A triangular (upper or lower right entires all zero),

$$det(A) = \text{ product of diagonal entries}$$

Find determinant using cofactors

What's det(A)?

$$\begin{bmatrix} 2 & -1 & 1 & 0 \\ 3 & 5 & 0 & -2 \\ 1 & 1 & 0 & -3 \\ 4 & 0 & 3 & -1 \end{bmatrix}$$

Easiest to go down the third column (b/c of the zeros):

det(A) = $1^{1+3} * 1$ det($\begin{bmatrix} 3 & 5 & -2 \\ 1 & 1 & -3 \\ 4 & 0 & -1 \end{bmatrix}$)+0 + 0 + $(-1)^{4+3} * 3$ det($\begin{bmatrix} 2 & -1 & 0 \\ 3 & 5 & -2 \\ 1 & 1 & -3 \end{bmatrix}$) = -50 + 99 = 49.

Chapter 12: Modules over PID

A $\mathbb{Z}$-module is an **abelian group**.
Thus,

$$\mathbb{Z}\text{-module} = \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \dots$$

by FTFGAG

Any $n\mathbb{Z}$ is an **ideal** of $\mathbb{Z}$ (the ideals are precisely $n\mathbb{Z}$).

The idea is to **generalize** the above by replacing $\mathbb{Z}$ with any PID, R.

in context of linear algebra

for vectors space V with a linear transformation A, we find a **different basis**.
This means we find B such that $B = P^{-1}AP$ for some matrix P.
This allows us to write transformation in **unique forms**:

- **Jordan Canonical** Form: as close to a diagonal matrix as possible
  - requires eigenvalues to be in field F.
- **Rational Canonical Form**: similar but doesn't require eigenvalues to be in F.

1 Fundamental Theorem of Finitely Generated Modules

(FTFGM) over PIDs
recall, PID = integral domain (commutative ring with unit and no zero divisors) where every ideal is principal.

For,
R = PID
M = finitely generated R-module.

There are two ways of **uniqely** decomposing a finitely generated module M:

1. Invariant Factor way:

$$M = \underbrace{R \oplus \cdots \oplus R}_{\text{rank r}} \quad \oplus \quad \underbrace{R/(r_1) \oplus \cdots \oplus R/(r_n)}_{invariant factors}$$

   where $r_1 | r_2 | \dots | r_n$.

2. Elementary Divisor way:

$$M = \underbrace{R \oplus \cdots \oplus R}_{\text{rank r}} \quad \oplus \quad \underbrace{R/(p_1^s) \oplus \cdots \oplus R/(p_n^s)}_{elementary divisors}$$

   where $p_1, p_2 \dots$ are prime elements (not necessarily distinct).

*recall: $p \in R$ is **prime** if (p) is a **prime ideal** (ab in (p) $\implies$ a or b in (p)); implies traditional def: $p|ab \implies p|ap|b$.

*recall: $A \oplus B = \{(a, b) : a \in A, b \in B\}$.

proof after Chineses Remainder and Noetherian R-modules

Note: Fundamental TFG Modules $\implies$ FTFGAG.

Chinese Remainder Theorem for R-modules

Let R be commutative with 1.
For A, B **comaximal** ideals in R,

$$A \cap B = AB \text{ and } R/AB \cong R/A \oplus R/B$$

comaximal means $A + B = R$ " sum gives entire ring." proof in notes

Noetherian R-Modules

M is a Noetherian R-Module is equivalent to any of the following:

- M satisfies ACC on R-submodules
- Every R-submodule is finitely generated

- Every collection of submodules has a maximal element

(eerily similar to Noetherian ring)

$\boxed{\begin{array}{l} M \text{ is Noetherian} \iff M'' \text{ and } M' = M/M'' \text{ are Noetherian} \\ \text{"submodules and quotients of Noetherian are Noetherian"} \end{array}}$

proof

Torsion

For R integral domain and M an R-module,

$$Tor(M) = \{x \in M : rx = 0 \text{ for some r } \in R\}$$

*M is torsion free if Tor(M) = 0

Annihilator of M is the ideal of R such that

$$Ann(N) = \{r \in R : rn = 0 \text{ for all n} \in N\}$$

2 Rational Canonical Form

Eigenvalue

The **eigenspace** of a linear transformation T is

$$\{v \in V : T(v) = Av = \lambda v\}$$

The **characteristic polynomial** of T, denoted $Ch_A(x)$ is det(xI - A).
often written A - xI, but above produces a nice monic polynomial.
degree n of $Ch_A(x)$ is the **dimension of V**.
The set of eigenvalues is precisely the set of **roots of the characterstic polynomial.** (at most n eigenvalues)

Minimal Polynomial

The unique monic polynomial, $m_A(x)$, of **smallest degree** such that $m_A(A) = 0$.
–can also think of $m_A(x)$ as **generator of Ann(V)** in $F[x]$

The minimal polynomial is the **largest invariant factor** (all invariant factors divide $m_A(x)$).

Characteristic Polynomial

- characteristic polyn is the **product** of all invariant factors

- **Cayley Hamilton**: min poly **divides** char poly

- char divides some power of the min polyn (meaning char and min have same roots)

SAME Charactersitic polynomial is a **necessary** but **not sufficient** condition to conclude two matrices are similar (they need to have the same RCF or JCF)

Companion Matrix of a polynomial

For any $a(x) \in F[x] = x^k + b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \cdots + b_0 0$,
the **companion matrix** of $a(x)$ is

$$\begin{bmatrix} 0 & 0 & \dots & -b_0 \\ 1 & 0 & \dots & -b_1 \\ \dots \\ 0 & 0 & \dots 1 & -b_{k-1} \end{bmatrix}$$

Rational biz

A matrix is in **rational canonical form** if the companion matrices of some polynomials $a_1(x)|a_2(x)|\dots|a_m(x)$ form the matrix.
"$a_i(x)$ are the **invariant factors**"

RCF of any matrix is **unique**

Two matrices are similar if and only if they have the **same RCF**.

To find all similar matrices, consider different possible minimal polynomials and invariant factors.

3 Jordan Canonical Form

Jordan form is as **close** as possible to a **diagonal matrix** (often simpler matrix than rational form).

To obtain the JCF, we use the **elementary divisor form** of the fundamental theorem.

Suppose for an $F[x]$-module of V with invariant factors $a_1(x)|a_2(x)|\dots|a_m(x)$, all monic polynomials. Then, the **elementary divisors** are powers of $(x-\lambda)^k$ (under the assumption the field F contains all eigenvalues of A).

The k x k **elementary Jordan matrix** with eigenvalue λ is

$$\begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0\dots & 0 \\ \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{bmatrix}$$

Jordan Canonical Form is a block diagonal matrix (square matrices along diagonal, zero elsewhere) with Jordan Blocks (above) along the diagonal.

unique up to permuting the Jordan Blocks.

Theorem if A contains all eigenvalues, then A is **similar to** a matrix in Jordan Canonical Form (JCF $= P^{-1}AP$ for some P).

$$\boxed{\text{A similar to JCF} \iff m_A(x) \text{ has no repeated roots}}$$

$$\boxed{\text{dim of eigenspace} = \#\text{ invariant factors} = \#\text{ Jordan Blocks}}$$

$$\boxed{\text{A can be } \textbf{diagonalized} \iff \text{Jordan blocks are of size 1}}$$

equivalent ot $m_A(x)$ having distinct roots

For matrices of size 2 or 3, knowing $m_A(x)$ and $ch_A(x)$ determines JCF.

For larger matrices (say 4x4), we can use **rank** to computer Jordan Blocks:

$$\boxed{\#\text{ Jordan Blocks of size k} = r_{k-1} - 2r_k + r_{k+1}}$$

where r = rank of matrix computed as rank $(A - I)^k$ (which is the number of linearly independent rows/columns.

e.g., number of Jordan blocks of size 2 $= r_1 - 2r_2 + r_3$ (compute $(A - I)^0 = I$ has rank 4 (for A 4x4), $(A - I)^1$ see # of independent rows ..)

computing JCF

1. Put charactersitic polynomial into form: $(x - \lambda)^k$
   (if can't, we won't be able to put into JCF)
2. size of JB for $=$ dim null space (A - λI)?

Linear fact $\boxed{\text{dim null space + dim column space (rank, = row space) = n}}$

Exercises

1. What are the submodules of $\mathbb{R}[x]$ for $V = \mathbb{R}^2$ and T : rotation (counterclockwise) by $\pi/4$?
   possibilities are dimension 0: point at center
   dimension 1: lines thorugh the center
   dimension 2: entire plane

   dimension 1 is not closed when rotating a point by $\pi/4$.
   So, 0 and whole thing are only submodules.
2. How about for S : rotation by π?
   0, lines through the origin, and whole plane
3. Is M = set $\mathbb{R}^2$ with T : rotation by π inside $\mathbb{R}[t]$-module cyclic? No, think polynomial $a + bt + ct^2$ acts by multiplication where $tv = T(v)$.
   Span of v, tv, t^2v, t^3v doesn't yield all of $\mathbb{R}^2$.

4. How about with T : rotation by $\pi/4$? yes!, v = (1, 0, then $T^2(v) = (0, 1)$ which spans all of $\mathbb{R}^2$.

5. Show A, B similar matrices have the same charactersitic polynomial.
$ch(B) = det(xI - B) = det(xI - P^{-1}AP) = det(P^{-1}xP - P^{-1}AP)$
$= det(P^{-1})det(x - A)det(P) =$ det(x - A).

6. Show the constant term in the characteristic polynomial of A (nxn) is $(-1)^n detA$. char poly = det(xI - A). The constant term is where $x = 0$, so we have constant term = det(-A) = $(-1)^n det(A)$ (depending on n even or odd)

7. Show the coefficient of A is the negative of trace(A). Note product of the diagonal: $(x - a_1)(x - a_2) \ldots (x - a_n)$; unclear

Chapter 13: Field Extensions

Goal: if $a(x)$ has no roots in F, how do we enlarge F so $a(x)$ has a root?

an element c is **algebraic** over F if it is the root of some nonzero polynomial in $F[x]$.(else it's **transcendental**)

a field K is **algebraically closed** if every polynomial $f(x) \in K[x]$ has at least one root in K.

recall: $F[x]$ is a ring, a particularly nice ring: Euclidean Domain.
Thus, every ideal in $F[x]$ is principal since $F[x]$ is a Euclidean Domain, hence a PID

Extensions as a Map over Polynomials

Consider

$$\varphi_c : F[x] \to F \text{ by } a(x) \to a(c)$$

φ_c is a homomorphism!

- Ker(φ) is an **ideal**, so it must be principal
  - it's generated by the minimum* polynomial of c
- Image(φ): turns out to be a field!
  - it's the **smallest field** containing F and c; call it $F(c)$.

– Image(φ) $\cong \frac{F[x]}{<m(x)>}$

*the **minimum polynomial** $p(x)$ of c over F is the polynomial of lowest degree in $F[x]$ such that $p(c) = 0$ (note by making $p(x)$ monic, we can ensure it's unique).

Any homomorphism $\varphi : F_1 \to F_2$ between fields is an **isomorphism** (or 0 map).

Extensions as Vector Spaces

For $F \subseteq K$, K can be thought of as a vector space over F.

The degree of K is denoted $[K : F]$.

It turns out $F(c) = span\{1, c, \ldots, c^{n-1}\}$ where n is the degree of the **minimal polynomial**.

proof: take any $a(c) \in F(c)$, then $a(x) = q(x)m(x) + r(x)$.
Evaluate at c, then $a(c) = 0 + r(c)$ where $r(c)$ has degree ¡ n.

Furthermore,

$$[E : F] = [E : K][K : F]$$

*when $[E : F] = n, [K : F] = m$ with $gcd(n, m) = 1$, $[EK : F] = nm$.

Any polynomial of degree n in $F[x]$ has **n roots** in an extension of F.

proof idea: the extension is $\frac{F[x]}{(p(x))}$, where $p(x)$ is the irreducible polynomial in F. This extension is a field by the work above, where a root c of $p(x)$ exists

If both a, b are roots of some irreducible $p(x) \in F[x]$, then

$$F(a) = \frac{F[x]}{(p(x))} = F(b)$$

implying a, b are **algebraically indistinguishable!**

α **algebraic** over F $\iff$ $F(\alpha)/F$ is finite degree extension.

α, β algebraic: carries over sums, products, division: $\alpha + \beta$ algebraic etc.

algebraic closure of a filed, say $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$, is $\mathbb{Q}$ plus all algebraic elements in $\mathbb{Q}$.

Every element of a **finite** field is algebraic

Take $F \subseteq K$ and $c \in K$ (deg k =n), then $1, c, \ldots, c^n$ is a linearly dependent set. Thus, $a_0 + a_1c + a_2c^2 + \cdots + a_nc^n = 0$ for some $a_i \in F$.

Every Finite extension is a **simple** extension (adjoins one element)

Characteristic of a field

The smallest number n such that $\underbrace{1+\ldots 1}_{n} = 0$

(else ch(F) = 0, if no finite n exists, e.g. $\mathbb{Q}$)

Note $ch(F)$ must be **zero** or **prime** (if not prime, then ab = 0, implying a=0 or b=0, a contradiction of requirement for ch to be smallest!)

so finite fileds must have **prime order!**

In characterstic p,

$$(a+b)^p = a^p + b^p$$

"against every inclination"

Splitting Fields

For $f(x) \in F[x]$, K is called a **splitting field** for $f(x)$ if

- $f(x)$ has all its roots in K ($f(x)$ splits into linar factors in K)
- it's the smallest such extensions (no subextension of K contains all roots of $f(x)$)

a polynomial is called **separable** if it has distinct roots in some splitting field. (if polynomial a repeated root, it's **inseparable**)

$$\boxed{\text{f(x) has distinct roots} \iff (f(x), d/dx f(x)) = 1}$$

α is a root of $f'(x) \iff$ is a multiple root of $f(x)$, thus minimal polynomial divides both f and f', meaning gcd $\neq 1\square$

$$\boxed{\text{ch(F)} = 0 \implies \text{any irred p(x) has \textbf{distinct} roots}}$$

why? if α is a multiple root of $p(x)$, then $p'(x)$ would have the same root and be of lower degree!

$$\boxed{\text{Splitting fields are unique}}$$

proof: division algo and induction by looking at map between two splitting fields to show they're iso

What's the degree of K over F ($[K : F]$)?

Suppose $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$. Then, $F(\alpha_1)/F \leq n$, $(\alpha_1, \alpha_2)/F \leq n-1$, etc.

Since, degree of extensions are multiplicative, $[K : F] \leq n!$.

For K_1, K_2 extensions of F of degrees n and m,

$$[K_1 K_2 : F] = nm \qquad \text{(if (n, m) = 1)}$$

If $p(x)$ irred in $F[x]$ has one root in a splitting field K, it must have **all its roots** in K.

Roots of Unity

The nth **roots of unity** in a field are elements a_i such that $a_i^n = 1$. the roots of unity divide a unit circle into arcs of equal length.

a is a **primitive nth root** of unity if n is the **smallest** integer such that $a^n = 1$.

Cyclotomic Polynomials

The nth **cylotomic polynomial** is

$$\Phi_n(x) = \prod_{1 \leq k \leq n, (n,k)=1} (x - e^{\frac{2i\pi k}{n}})$$

For n prime,

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1}$$

For $n = 2p$,

$$\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1}$$

The first few cyclotomic polynomials are

$$\Phi_1(x) = x - 1 \Phi_2(x) = x + 1 \qquad \Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1 \Phi_5(x) = x^4 + x^3 + x^2 + x + 1 \qquad \Phi_6(x) = x^2 - x + 1.$$

$$\boxed{\text{The degree of } \Phi_n(x) = \varphi(n)}$$

The cyclotmoic polynomial $\Phi(n)$ is the **minimal** polynomial of any nth root of unity ζ_n.

Cyclotomic Fields

Field obtained by joining any primitive nth roots of unity.
For any field F, $F(\zeta_n)$ is called a **cylotomic field** for ζ_n the nth root of unity. The field is **cylic** !

Exercises

1. What is $(1 + \sqrt[3]{2})^{-1}$ in $\mathbb{Q}(\sqrt[3]{2})$?
   1. min poly is p(x) = $x^3 - 2$, since $\sqrt[3]{2}$ is a root and p(x) is irreducible by Eisenstein.
   2. Thus, $\mathbb{Q}[x]/p(x) = \mathbb{Q}(\sqrt[3]{2}$.
   3. Inside field, $p(x)$ is zero.

   idea: use euclidean algo to find $a(x)(1 + x) + b(x)(x^3 - 2) = 1$.
   evaluate $a(x)$ at α to find inverse of $(1 + \alpha)$, since right term goes to zero!

2. What is $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$?
   min poly: $x^n - 2$, so degree of extension is n.

3. What's the degree of the splitting field for $(x^2-2)(x^2-3)$?
   It's the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, which by previous work is 4.

4. What's the degree of $\mathbb{Q}(\sqrt[4]{2}, \sqrt{2})$?
   it equal to the degree of $\mathbb{Q}(\sqrt[4]{2})$

5. For $p(x) = x^3 + 9x + 6$ and θ a root, find $\frac{1}{1+\theta} \in \mathbb{Q}(\theta)$.
   since $p(x)$ is irreducible, we know

   $$a(x)(1+x) + b(x)(x^3 + 9x + 6) = 0$$

   by gcd. At $x = \theta$, $a(\theta)(1+\theta) + 0 = 0$, meaning $a(\theta)$ is the inverse we seek.
   To find $a(x)$ use Euclidean algo.

6. In general to find θ^{-1}, consider factoring θ as in page 516 of Dummit.

Strategies:

- To find minimal polynomial, try multiplying out complex conjugates of root given (x - root)(x - complex conju of root). Hopefully polynomial is irreducible , done.

- Another way to determine degree is to take something like $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ show it equals a simpler field ($\mathbb{Q}(\sqrt{2})$ in this case) by squaring the element.

Field Automorphisms and Galois

$$Aut(K/F) = \{\sigma \in Aut(K) | \sigma \text{ fixes } F\}$$

Automorphisms of K/F only take **roots to roots** of same poly.

$$\boxed{|Aut(K/F)| \leq [K : F]}$$

(equality if the polynomial of the splitting field is **separable**)

A field extension K is **Galois** only if $|Aut(K/F)| = [K : F]$.
Since automorphisms of a splitting field K of $p(x)$ permute roots of $p(x)$,

$$|Aut(K/F)| = [K : F] = \text{degree of K over F}$$

e.g., $2 = |Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})|$ since autmorphisms can take $\sqrt{2}$ to itself or $-\sqrt{2}$.

e.g., $4 = |Aut(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})|$ similar argument with options for both $\sqrt{2}$ and $\sqrt{3}$.

Automorphisms as a Group: Galois Groups

$$\text{Gal(K/F)} = \text{permutations of roots of } a(x) = \text{Aut(K/F)}$$

(not every permutation; just ones uniquely identifying an automorphism)

These automorphisms are a group, called the **Galois Group**, under composition.

Fixed Fields

For K a splitting field of $p(x)$ over F, one-to-one between

$$\boxed{\text{subgroups of Gal(K/F)} \iff \text{subfields of } K}$$

e.g., what's the splitting field of $x^p - 2$ over $\mathbb{Q}$?

roots are $\sqrt[p]{2}, \zeta_p \sqrt[p]{2}, \ldots \zeta_p^{p-1} \sqrt[p]{2}$ which are contained in $\mathbb{Q}\sqrt[p]{2}, \zeta_p$.

Review Galois Theory

- For $p(x) \in F[x]$ **irreducible**, then $p(x)$ has a root in some extension of F.
- For α a **root** of $p(x)$, $F(\alpha) \cong \frac{F[x]}{(p(x))}$.
  - if α, β roots of $p(x)$ $F(\beta) \cong F(\alpha)$ "algebracailly indistinguishable"
- $[F(\alpha) : F]$ = degree of minimal polynomial
- a homomorphism between fields is an isomorphism or 0.
- **quadratic extensions** equivalent to adjoining $\sqrt{D}$ (square-free)
- K_1K_2, **composite extension**, is the smallest field containing K_1, K_2.
  - $[K_1 : F] = n, [K_2 : F] = m$, then $[K_1K_2 : F] \leq nm$ (= if (n, m)=1).
- a field K is **algebraically closed** if every poly in $K[x]$ has a root in K. (this in fact means every root of any poly is in K by factoring argument)
- the **splitting field** K of a polynomial is the smallest field containing all its roots.
  - for K splitting field, $[K : F] \leq n!$
- $f(x) \in F[x]$ is **separable** $\iff$ $(f(x), f'(x)) = 1$.
- In $ch(F) = 0$ or for F finite field,
  - $p(x)$ irreducible $\implies$ $p(x)$ is separable.
  - $p(x)$ is separable $\iff$ $p(x)$ is the product of distinct irreducibles.

Questions:

- Does $\zeta_n = e^{2\pi i/n}$?