Exam Tips

** are statements not proved in lectures

Basics of Rings

Always remember there are TWO steps to prove two sets are the same: A⊆B, B⊆A

- e.g. when proving Ker(f) = N

Checking S is subring of R:

- 0_R, 1_R ∈ S
- +, x closed in S

Properties preserved under subring:

- commutativity
- integral domain

C is field, but subring Z[√(-5)] is not even UFD. So subring will NOT preserve: UFD, PID, ED, field.

ALWAYS remember to consider the edge cases:

- trivial ring {0}
- zero-ideal (0) = {0}
- trivial ideal R

Unless n is prime, Z_n is NOT F_n, because F_n need a structure that makes it a field.

When infinite sum is involved, we often require only finitely many terms to be non-zero (finite support)

- when integrals are considered, the condition compact support is used.

Polynomials should NOT be seen as functions

- different polynomials can lead to the same function

In group ring, the group operation is treated as multiplication in ring

Check a set is ideal:

- Check it is kernel of a ring homomorphism.
- Subgroup + closed under multiplication by R

building new ideal:

- intersection of any set of ideals is ideal
- infinite union of ASCENDING ideals is ideal
    - NOT true for union of any set of ideals

warning: Image of ideal under homomorphism may NOT be ideal

- but for surjective homomorphism, ideal will be mapped to ideal

Many uniqueness are up to associate!!

- Irreducible elements is still irreducible under multiplication of unit
- unique factorisation domain: irreducible factors unique up to associates.
- on UFD, gcd is only unique up to associates.
- Diagonal elements of Smith normal form: unique up to associates.
- content of polynomial is unique up to associates.
- content c(fg) may not be c(f) c(g), but they are associates

There are rings of non-prime characteristics, but they are not integral domains.

- e.g. char(Z_4) = 4

When using first isomorphism theorem, RHS is Im(f). Have to check SURJECTIVITY if want to use on the whole ring.

Ideal extension, contraction

given ring homomorphism f : A→ B, and ideal I, J of A, B respectively

f(I) may NOT be ideal (unless f is surjective)

- the ideal generated by f(I) is called ideal contraction of I, written as I^e

f^{-1}(J) must be an ideal, it is called contraction of J

- further, image of generating set of f^{-1}(J) is generating set of J

Given ideal I in R, you can always create ideal I + (X) in R[X]   (check this is ideal!)

- set of polynomials with coefficients in I is also an ideal in R[X]. And this ideal J satisfies I = J∩R

all ideals J in S^{-1}R looks like S^{-1}I where I is ideal in R.

I = {r : r/1 ∈ J}

Prime, irreducibility

Unit elements are not irreducible nor prime maximal ideal and prime ideal can be {0}, but NOT R (non-trivial)

- maximal ideals are always prime (R commutative)
- non zero prime ideals are maximal in PID

meanwhile

- every prime element is irreducible (in ID)
- every irreducible is prime in PID

R is commutative ring, $r \neq 0$

$$\begin{tikzcd}
\text{(r) prime} \arrow[r, leftrightarrow] & \text{r prime} \arrow[d, phantom, "????"] \\
\text{(r) maximal} \arrow[u] \arrow[r, phantom, "????"] & \text{r irreducible}
\end{tikzcd}$$

R is Integral Domain, $r \neq 0$

$$\begin{tikzcd}
\text{(r) prime} \arrow[r, leftrightarrow] & \text{r prime} \arrow[d] \\
\text{(r) maximal} \arrow[u] \arrow[r] & \text{r irreducible}
\end{tikzcd}$$

R is UFD, $r \neq 0$

$$\begin{tikzcd}
\text{(r) prime} \arrow[r, leftrightarrow] & \text{r prime} \arrow[d, leftrightarrow] \\
\text{(r) maximal} \arrow[u] \arrow[r] & \text{r irreducible}
\end{tikzcd}$$

R is PID, $r \neq 0$

$$\begin{tikzcd}
\text{(r) prime} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \text{r prime} \arrow[d, leftrightarrow] \\
\text{(r) maximal} \arrow[r, leftrightarrow] & \text{r irreducible}
\end{tikzcd}$$

Warning: (0) may not be prime, unless on integral domain

PID, UFD

Z is PID, Z[i] is PID, but Z[X] is not PID e.g. (2, X) is not PI

Z/nZ is PIR (all ideals are principal but the ring is not ID), but Z/pZ is PID, Z/pZ[X] is PID iff p is prime, because:

** R[X] is PID ⇔ R is field

- If R[X] is PID, take any element r of R, consider the ideal (r, X)
- If R is field, long division of polynomials is possible. So for any field F, F[X] is ED

Noetherian ⇔ All ideals are finitely generated

If R is field, R[X] is PID, so ideal I = (f, g) = R[X] if f, g has no common factor

Even if F is field, F×F is not field. As (0, 1) has no inverse.

It is more difficult to prove a ring is not Euclidean domain, so usually first check if it is PID.

Constructing Rings

Given a “norm” function N : R → S s.t. N(ab) = N(a) N(b) and N(1) = 1, then $N(R^x) \subseteq S^x$

- so norm of unit must be a unit in S.
- e.g. When S is Z and image of N is non-negative, norm of unit in R must be 1.

you can also use norm to prove irreducibility, and invertibility.

Factorisation on polynomial ring

R assumed to be UFD for most of this part, polynomials are on R[x]
Properties inherited by R[X] from R

- Commutativity
- ID (no zero divisor)
- UFD
- Noetherian (Hilbert basis theorem)
- ** characteristic n

justify primitivity of polynomial when you are using:

- Eisenstein’s criterion,
- Gauss lemma
- for non-primitive constant, simply take out the content, i.e. f = c(f) f_1 where f1 is primitive.

content c(f) is only well-defined up to a unit

- as gcd is only unique up to unit
- if f = cf′ where f′ is primitive, c(f) is NOT c but uc for some unit u.

deg(fg)=deg(f)+deg(g) ONLY holds in ID !!!

fg is primitive ⇔ f, g are primitive

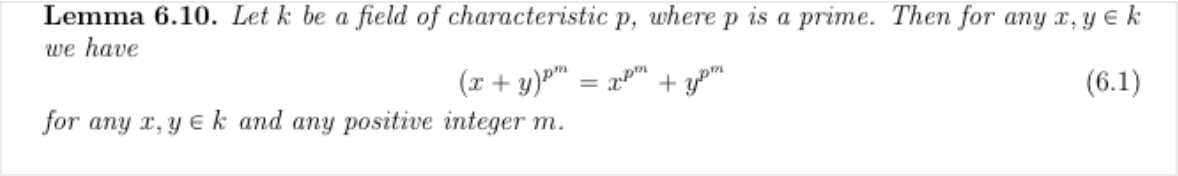
- generally, factors of primitive are primitive

Use general version of Eisenstein’s criterion on rings like Q[x, y]

- instead of divisibility, argue using prime ideal.

if Eisenstein’s criterion fails, try simple substitutions like Y = X-1
and note Eisenstein criterion fails if R is field, because there is no irreducible element in a field.

useful factorisation formulae on finite field



Lemma 6.10. *Let k be a field of characteristic p, where p is a prime. Then for any $x, y \in k$ we have*

$$(x+y)^{p^m} = x^{p^m} + y^{p^m} \tag{6.1}$$

for any $x, y \in k$ and any positive integer m.

to prove polynomial has no linear factor over R[X], you must prove it has no roots in Frac(R)[X]. Because if r/s is a root, (sx-r) is a linear factor.

- rational root theorem may help here

field of fractions of both Q[X], Z[X] are Q(X)

Local rings

On local rings, or any ring with division, check DENOMINATOR is NONZERO!

natural injection ι is injective(i.e. R is subring of $S^{-1}R$) iff R is ID

zero element in local ring is (0, 1), NOT (0, 0)

Algebraic numbers and Noetherian Rings

algebraic integer: numbers in C that are roots of MONIC polynomial in Z[X]
algebraic number: numbers in C that are roots of non-zero polynomial in Z[X]
this course mainly discuss algebraic integer.

check algebraic integer or not:
the only algebraic integers in Q are Z

- you may use this fact and algebraic rules of algebraic integers to prove some number is not algebraic integer.

Find the of polynomial sending α to 0:
simply compute α, α^2, α^3, ... and see if you find make things 0.

- remember to recognise roots of unity, it is an easier case
- if you can write some terms in α^n by α (or any lower degree term), that would be very helpful.

to prove the polynomial you found is minimal, you should prove it is irreducible

- rational root theorem may help for low degrees (if no rational root, no linear factor in Z[X])

    - otherwise you can try to factorise in C to prove factorisation in Z[X] is not possible.
        - Note: Z[i] is UFD

rational root theorem: if R is UFD, F = Frac(R), if a polynomial f in R[X] has root p/q (gcd(p, q) = 1), then p divides constant term, q divides leading coefficient of f.

- corollary: if f is monic, all roots in F are in R

converse of Hilbert basis theorem is true, so actually
R Noetherian ⇔ R[X] Noether ian
R Noetherian ⇒ $S^{-1}R$ is Noetherian

Field

Useful characterisation of field: only ideals are {0}, R

homomorphism from field to non-zero ring must be injective

Modules

submodules of finitely generated modules may NOT be finitely generated

- Let R = $Z[X_1, X_2, \dots]$ take R-module R and submodule $Z[X_1X_2, X_1X_3, \dots]$, not finitely generated
- Corollary: f.g. ideals may contain non f.g. ideals.

when the left/right R-module R itself is taken, submodules are the left/right ideals of R.

R-module M with R-action is determined by map R → End(M)

some properties from linear algebra fails, e.g.

- spanning set for module may not contain basis
- LI set in module may not be able to extend to a basis

trivial module {0} is a free-module of rank 0

submodules of free/projective module may not be projective

- Let R = K[X, Y], use R-module R (which is clearly free R-module), submodule (X, Y) is not projective.

singleton set may still be linear dependent (when the element is a zero divisor)

Examples

examples from lecture notes that we can use:

$M_n(R)$ not commutative for any n > 1, R≠{0}

given matrix A, and field F, on polynomial ring, ideal {f ∈ F[X] : f(A) = 0} is principal (as F[X] is PID), so I = (m) and m is called minimal polynomial.

Q : prime field (no subfield smaller than itself)
Z[i]: ED but not field, ϕ(z) = $|z|^2$
Z[X]: UFD but not PID
Z[√(-5)]: ID but not UFD
Z/6Z: Noetherian but not ID

non-Noetherian rings:

- ring of continuous functions on [a, b]
- $K[X_1, X_2, \dots]$ (infinite-variable polynomials over K)

C[X] / (X) ≅ C
for a > 0

- R[X] / (X^2+a) ≅ C
- R[X] / (X^2-a) ≅ R x R
- R[X] / (X^2) ≅ ring of dual numbers