Section 11.7 – Fields of Fractions

Construction (fractions out of a domain). For an integral domain R set

$$\mathrm{Frac}(R) = \left\{ \tfrac{a}{b} \mid a, b \in R,\ b \neq 0 \right\} \big/ \sim, \qquad \frac{a}{b} \sim \frac{c}{d} \iff ad = bc.$$

Addition $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ and multiplication $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ make it a field. The natural map $R \hookrightarrow \mathrm{Frac}(R)$ sends $a \mapsto a/1$.
Why care? Every domain can be "upgraded" to a field so we can divide by non-zero elements during proofs and computations.
When to use: Turning lemmas proved in R into field statements or vice versa.

Walk-through Example 1

Question. Show that the only integers that turn into units (invertible elements) inside $\mathbb{Z} \hookrightarrow \mathbb{Q}$ are ± 1.
▷ Recall definition: a unit u satisfies $uu^{-1} = 1$.
▷ In $\mathbb{Q}$, the inverse of an integer $n \neq 0$ is $1/n$.
▷ $1/n \in \mathbb{Z} \implies n = \pm 1$. (All other inverses are non-integral.)

Section 12.3 – Gauss's Lemma

Primitive polynomial. A non-zero $f = \sum a_k x^k \in R[x]$ is *primitive* if $\gcd(a_0, \dots, a_n) = 1$ in R.
Why care? "Primitive" means "coefficients share no common factor" — handy for irreducibility tricks.
Gauss's lemma (UFD version). If R is a UFD then
- the product of two primitive polys is primitive;
- f is irreducible in $R[x] \iff f$ is primitive *and* irreducible in $\mathrm{Frac}(R)[x]$.

When to use: Proving irreducibility over $\mathbb{Z}$ by reducing to $\mathbb{Q}[x]$ or finite fields.

Walk-through Example 2

Show $x^3 + 2x + 2 \in \mathbb{Z}[x]$ is irreducible.
▷ Check primitivity: coefficients $1, 0, 2, 2$ have gcd $= 1$.
▷ Reduce mod 2: $x^3 + 2x + 2 \equiv x^3$ in $\mathbb{F}_2[x]$.
▷ Over $\mathbb{F}_2$, the only linear factor of x^3 is x, but that leaves x^2, which is not a new non-unit factor.
▷ Hence no degree-1 factor irreducible in $\mathbb{Z}[x]$ by Gauss.

Section 12.4 – Eisenstein Criterion

Eisenstein. For $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$, a prime p with

$$p \nmid a_n, \quad p \mid a_k\ (k < n), \quad p^2 \nmid a_0$$

makes f irreducible in $\mathbb{Q}[x]$.
Why care? A quick irreducibility test—look for "one prime rules them all".

Three-step recipe

1) Clear denominators so $f \in \mathbb{Z}[x]$ and primitive.
2) Hunt for a prime p meeting Eisenstein's divisibility pattern.
3) Conclude irreducibility (or try a different p if needed).

Walk-through Example 3

Prove $g(x) = x^4 + 10x + 5$ is irreducible.
▷ Already primitive (gcd $= 1$).
▷ Try $p = 5$: coefficients $(1, 0, 0, 10, 5)$.
▷ Check: $5 \nmid 1$, $5 \mid 0, 0, 10$, $5^2 = 25 \nmid 5$. Criterion satisfied irreducible.

Section 14.1 – Basic Module Language

R-module. An abelian group M with scalar multiplication $R \times M \to M$ obeying distributive laws.
Why care? Generalises vector spaces where the "scalars" live in any ring R.
Key terms (quick list).
- **Submodule**: closed under + and scalar-mult.
- **Quotient**: M/N is the cosets of N.
- **Hom**: $\mathrm{Hom}_R(M, N)$ are R-linear maps.
- **Cyclic**: generated by one element, $M \cong R/I$.

Nakayama (nilpotent ideal form). If M finitely generated and $JM = M$ for a nilpotent ideal J ($J^k = 0$), then $M = 0$.
When to use: Recognising "nothing hides inside" when a nilpotent ideal acts surjectively.

Mini-exercise 4 (submodules in $\mathbb{Z}_8$)

Take $R = \mathbb{Z}_8$, $M = R$.
▷ $2M = \{0, 2, 4, 6\}$ — not everything $2M \neq M$.
▷ $4M = \{0, 4\} \subsetneq 2M$. Visualise $4M \subset 2M \subset M$.

Matrices over General Rings

$M_{n\times m}(R)$. $n \times m$ matrices with entries in R.
Why care? Lets us transport linear-algebra intuition to non-field coefficients.
Determinant (square case). Multilinear, alternating map $\det : M_n(R) \to R$ with $\det I = 1$.
Substitution trick. Prove identity over the polynomial ring $\mathbb{Z}[t_{ij}]$, then substitute.
Cayley–Hamilton. Every square matrix over a commutative ring annihilates its own characteristic polynomial $p_A(t)$.
When to use: To bound powers of A, prove minimal polynomials, etc.

Walk-through Example 5

Show $\det(A)\det(B) = \det(AB)$ for integer matrices.
▷ Work in $R = \mathbb{Z}[\{t_{ij}\}, \{s_{ij}\}]$.
▷ Use the usual cofactor-expansion proof.
▷ Substitute $t_{ij} \to A_{ij}$, $s_{ij} \to B_{ij}$.

Section 14.2 – Free Modules

Free module of rank n. Direct sum $R^{\oplus n}$ with basis $e_1, \dots, e_n$.
Why care? Acts like "$\mathbb{Z}^n$" or "F^n" but over any ring.
Universal mapping property. Giving images of the basis vectors completely determines an R-linear map out of a free module.

Walk-through Example 6

Why do any two bases have the same size?
▷ Suppose bases $\{e_i\}_{i=1}^n$ and $\{f_j\}_{j=1}^m$.
▷ Map $e_i \mapsto f_i$ (extend by 0 if $m > n$) to get a surjection $R^{\oplus n} \twoheadrightarrow R^{\oplus m}$.
▷ Surjection $m \leq n$. Swap roles $n \leq m$. Hence $n = m$.

Section 14.6 – Noetherian Rings

Noetherian. Every ascending chain of ideals eventually stabilises.
Why care? Guarantees there are "only finitely many generators" hiding in infinite-looking objects.
Hilbert basis theorem. If R Noetherian, then $R[x]$ is Noetherian.

Walk-through Example 7

Prove $\mathbb{Z}[x_1, \dots, x_n]$ is Noetherian.
▷ Base: $\mathbb{Z}$ is Noetherian (every ideal $\langle d \rangle$ is principal).
▷ Induction: assume $\mathbb{Z}[x_1, \dots, x_{k-1}]$ Noetherian.
▷ Apply Hilbert one more variable is still Noetherian.
▷ Reach $k = n$. Done.

Section 14.4 – Smith Normal Form (SNF)

For a PID R and $A \in M_{m\times n}(R)$, $\exists$ invertible U, V s.t.

$$UAV = \mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0), \quad d_i \mid d_{i+1}.$$

Why care? Diagonalising over $\mathbb{Z}$ or $F[x]$ reads off invariants for abelian groups or linear maps.

Walk-through Example 8

SNF of $\begin{pmatrix} 4 & 6 \\ 2 & 8 \end{pmatrix}$ over $\mathbb{Z}$.

▷ Row-reduce: subtract 2× row 2 from row 1 → $\begin{pmatrix} 0 & -10 \\ 2 & 8 \end{pmatrix}$.

▷ Swap columns: → $\begin{pmatrix} -10 & 0 \\ 8 & 2 \end{pmatrix}$.

▷ $\gcd(-10, 8) = 2$; perform column ops → $\begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix}$.

▷ Hence SNF is $\mathrm{diag}(2, 10)$.
▷ Module quotient $\mathbb{Z}^2/A\mathbb{Z}^2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/10$.

Sections 14.7–14.8 – Modules over a PID

Structure theorem. Every finitely generated R-module (PID) breaks into

$$R^{\oplus r} \oplus \bigoplus_i R/(p_i^{e_i}).$$

Why care? Master key for classifying finite abelian groups and rational canonical form.

Quick Corollaries

- Finite abelian group $\cong$ direct sum of p-power cyclic pieces.
- Any matrix over a field is similar to a block diagonal of companion matrices.

Walk-through Example 9

Classify groups of order $360 = 2^3 \cdot 3^2 \cdot 5$.
▷ Break into 2-, 3-, and 5-parts via CRT.
▷ 2^3-part: $\mathbb{Z}/8$, $\mathbb{Z}/4 \oplus \mathbb{Z}/2$, $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$.
▷ 3^2-part: $\mathbb{Z}/9$, $\mathbb{Z}/3 \oplus \mathbb{Z}/3$.
▷ 5-part fixed: $\mathbb{Z}/5$.
▷ Combine each 2-choice with each 3-choice and $\mathbb{Z}/5$.

Walk-through Example 10 (outline)

Rational canonical form for $A \in M_n(F)$.
▷ View F^n as an $F[x]$-module via $x \cdot v = Av$.
▷ Apply structure theorem to decompose into cyclic submodules.
▷ Translate each cyclic piece into a companion matrix block.

60-Second Reference Table

Topic	Mnemonic / What to remember
Field of fracs	"Clear denom → fractions behave like $\mathbb{Q}$."
Gauss lemma	Primitive + irreducible over field implies irreducible over ring.
Eisenstein	Find one prime doing all the divisibility work.
Modules basics	Think "vector spaces w/o division"; sub-/quotient; Nakayama kills nilpotent.
Determinant	$\det(AB) = \det A \det B$; Cayley–Hamilton $p_A(A) = 0$.
Free modules	Basis size is invariant; linear maps (double arrow) matrices.
Noetherian	"Chains stop"; Hilbert: add a variable, still stops.
SNF	PID-Gaussian elimination → diagonal divisibility chain.
PID modules	Free part + torsion part, unique shape.

Problem 1. Show that the ideal $(2, x)$ in $\mathbb{Z}[x]$ cannot be generated by a single element.
Key idea: Reduce mod 2 and compare generators.
Recipe:

1. Assume $(2, x) = (g(x))$ for some $g \in \mathbb{Z}[x]$.
2. Pass to $\mathbb{F}_2[x]$ by reducing coefficients mod 2; $(2, x)$ becomes (x).
3. A principal ideal $(\bar{g})$ equals $(x) \implies \bar{g} = u\,x$, where $u \in \mathbb{F}_2^\times$.
4. Lift back: $g(x) = xh(x) + 2k(x)$ with $h(0)$ *odd*.
5. Show $x \notin (g)$ by evaluating any combination $a(x)g(x)$ at $x = 0$.

Solution: Suppose $(2, x) = (g)$. In $\mathbb{F}_2[x]$ we have $(\bar{g}) = (x)$, so $\bar{g} = ux$ with $u \in \mathbb{F}_2^\times$. Hence $g = xh + 2k$ for some $h, k \in \mathbb{Z}[x]$ and $h(0)$ odd. If $x \in (g)$ there is $a(x) \in \mathbb{Z}[x]$ such that $a(x)g(x) = x$. Set $x = 0$:

$$0 = a(0)\,g(0) = a(0)\,2k(0) \quad \Longrightarrow \quad 2 \mid x$$

– impossible. Therefore $(2, x)$ is *not* principal. □

Problem 2. Let F be a field. Describe all ring homomorphisms $\varphi : F[x] \to F$ that restrict to the identity on F.
Key idea: A homomorphism out of a polynomial ring is determined by the image of x.
Recipe: Pick any $a \in F$ and define $\varphi_a(\sum c_i x^i) = \sum c_i a^i$.
Solution: For every $a \in F$, the "evaluation at a" map φ_a is a homomorphism and satisfies $\varphi_a|_F = \mathrm{id}$. Conversely, if φ is such a homomorphism, set $a := \varphi(x) \in F$; the universal property of $F[x]$ forces $\varphi = \varphi_a$. Thus the set of all homomorphisms is $\{\varphi_a \mid a \in F\}$. □

Problem 3. Let $A, B \in F^{n\times n}$ be diagonalizable. Is there always a single $P \in \mathrm{GL}_n(F)$ with PAP^{-1} and PBP^{-1} both diagonal?
Answer: *No.*
Counter-example (recipe):
- Take $F = \mathbb{R}$, $n = 2$.
- Put $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ (already diagonal).
- Put $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (diagonalizable via the Hadamard matrix).
- $AB \neq BA$; non-commuting diagonalizable matrices cannot be simultaneously diagonalized.

Problem 4. Same set-up as Problem 3, but assume $AB = BA$.
Key idea: Commuting diagonalizable matrices are simultaneously diagonalizable.
Recipe:

1. Work in an algebraic closure if needed.
2. Pick an eigenbasis of A; with $AB = BA$, each eigenspace of A is B-stable, so B acts on it and is diagonalizable there.
3. Repeat recursively to build a common eigenbasis.

Solution: There exists P whose columns form a joint eigenbasis; then PAP^{-1} and PBP^{-1} are both diagonal.
□

Problem 5. (Jordan/Chevalley decomposition) For $A \in \mathbb{C}^{n\times n}$, show $A = D + N$ with D diagonalizable, N nilpotent, and $DN = ND$.
Recipe:

1. Put $A = SJS^{-1}$, where J is the Jordan canonical form.
2. Split $J = \mathrm{diag}(\lambda_i) + N_J$ (strictly upper part is nilpotent).
3. Set $D = S\,\mathrm{diag}(\lambda_i)\,S^{-1}$, $N = SN_JS^{-1}$.

Solution: D is similar to a diagonal matrix ⇒ diagonalizable. N_J is nilpotent ⇒ N nilpotent and nilpotent Jordan parts commute, so do D and N. Uniqueness follows from spectral projectio
Problem 6. Let $f\colon V \to V$ be linear and define $f \oplus f$ on $V \oplus V$ by $(f \oplus f)(v, w) = (f(v), f(w))$.

(a) **Triangularizability.** $f \oplus f$ is upper triangularizable ⇔ f is, because the block matrix $f0$ $0f$ has the same Jordan blocks as f (just doubled).
(b) **Diagonalizability.** Same reasoning: $f \oplus f$ diagonalizable ⇔ every Jordan block of f has size 1 ⇔ f diagonalizable.
(c) **Jordan blocks.** Each Jordan block $J_k(\lambda)$ of size k for f gives *two* identical blocks $J_k(\lambda)$ for $f \oplus f$.

Problem 7. Units in $(\mathbb{Z}/4\mathbb{Z})[x]$.
Key idea: In $R[x]$ a polynomial is a unit iff its constant term is a unit in R and the remaining coefficients are nilpotent.
Recipe:
- Units of $\mathbb{Z}/4\mathbb{Z}$ are $1, 3$; nilpotent element is 2 (since $2^2 = 0$).
- Write $f(x) = u + 2g(x)$ with $u \in \{1, 3\}$, $g(x) \in (\mathbb{Z}/4\mathbb{Z})[x]$.

Answer:

$$(\mathbb{Z}/4\mathbb{Z})[x]^\times = \{\, u + 2g(x) \mid u \in \{1, 3\},\ g(x) \in (\mathbb{Z}/4\mathbb{Z})[x] \}.$$

Problem 8. Characteristic polynomial of a nilpotent matrix.
Answer & Reasoning: If N is $n \times n$ and nilpotent, its only eigenvalue is 0, so $\chi_N(t) = t^n$.