Algebra 2 Notes

by Tyler Wright

github.com/Fluxanoia fluxanoia.co.uk

These notes are not necessarily correct, consistent, representative of the course as it stands today, or rigorous. Any result of the above is not the author's fault.

These notes are in progress.

Contents

1 The Fundamentals

1.1 Rings (1.1)

A ring is a set with two binary operations, addition and multiplication, such that they are both commutative, associative, and addition is distributive over multiplication, so for a, b, and c in some ring:

$$(a+b)c = ac + bc.$$

We also have that rings must contain 'zero' and 'one' elements, the additive and multiplicative identities, and every element of the ring has an additive inverse.

1.2 Properties of Rings (1.3)

For a ring R with a, b, and c in R:

- if $a + b = b$ then $a = 0$, 0 is unique,
- if $a \cdot x = x$ for all x in R, then $a = 1$, 1 is unique,
- if $a + b = 0 = a + c$ then $b = c$, $-a$ is unique,
- we have $0 \cdot a = 0$,
- we have $-1 \cdot a = -a$,
- we have $0 = 1$ if and only if $R = \{0\}$.

1.3 Units (1.6-7)

For a ring R, with r in R, if there exists some s such that $rs = 1$ then r is a unit and $s = r^{-1}$ is the multiplicative inverse of r. We write $R^{\times}$ to be the set of all units in R, which is an abelian group under multiplication.

1.4 Fields (1.9)

A non-zero ring R is a field if $R \setminus \{0\} = R^{\times}$.

1.5 Subrings (1.14-15)

For a ring R, $S \subseteq R$ is a subring of R if it is a ring and contains zero and one. This is equivalent to saying S is closed under addition, multiplication, and additive inverses, and contains 1.

1.6 The Gaussian Integers (1.17, 1.19)

We define the Gaussian integers as:

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

which is the smallest subring of $\mathbb{C}$ containing i. Generally, for α in $\mathbb{C}$, $\mathbb{Z}[\alpha]$ is the smallest subring containing α and for a ring R with a subring S, for some β in R, we have $S[\beta]$ is the smallest subring of R containing S and β.

1.7 Product Rings (1.20)

For R and S rings, we have that $R \times S$ is a ring under component-wise addition and multiplication.

1.8 Distributivity of Taking Units (1.22)

For rings R and S, $(R \times S)^\times = R^\times \times S^\times$.

Proof. We consider:

$$\begin{aligned}(r, s) \in (R \times S)^\times &\iff (r, s)(p, q) = (1, 1) \text{ for some } (p, q) \in R \times S \\ &\iff rp = 1 \text{ and } sq = 1 \text{ for some } p \in R \text{ and } q \in S \\ &\iff r \in R^\times \text{ and } s \in S^\times,\end{aligned}$$

as required. □

1.9 Polynomials (1.23)

For a ring R and a symbol x, we have that the following is a ring:

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{Z}_{\geq 0}, (a_i)_{i \in [n]} \in R^n\}.$$

1.10 Ring Homomorphisms (2.7, 2.12)

For R and S rings, a map φ from R to S is a ring homomorphism if it preserves addition and multiplication. This implies that 0 and 1 are fixed points of φ and taking additive inverses is preserved by φ.

We have some properties of ring homomorphisms:

- $\varphi(0) = 0$,
- $\varphi(-a) = -\varphi(a)$,
- the image of φ is a subring of S,
- homomorphisms are preserved under composition.

1.11 Ring Isomorphisms (2.1)

A ring isomorphism is a bijective ring homomorphism.

1.12 The Kernel (2.13, 2.18)

The kernel of a homomorphism is the set of values it maps to 0. This is not necessarily a ring. The kernel is $\{0\}$ if and only if the homomorphism is injective.

1.13 Ideals (2.15-16)

For a ring R with $I \subseteq R$, I is an ideal if it is an additive subgroup of R and for all r in R and i in I, ri is in I. The kernel of homomorphisms are ideals.

1.14 Preservation of Satisfaction (2.20)

For a ring R with r in R, if for some n in $\mathbb{Z}_{\geq 0}$ we have $(a_i)_{i \in [n]}$ in $\mathbb{Z}^n$ such that:

$$a_n r^n + \cdots + a_1 r + a_0 = 0,$$

then for any homomorphism φ on R to some other ring S, we have that:

$$\varphi(a_n r^n + \cdots + a_1 r + a_0) = 0.$$

1.15 Cosets (2.22)

For a ring R with r in R and an ideal I of R, the coset of r modulo I is the set:

$$r + I = \{r + i : i \in I\}.$$

For each r and s in R, we define a relation by:

$$r \sim s \Longleftrightarrow r - s \in I,$$

which is an equivalence relation, with equivalence classes the cosets of R modulo I. Thus, cosets are either identical or disjoint.

2 Quotients

2.1 Quotient Rings (2.24-25)

The set of cosets modulo I of a ring R forms a ring, the quotient ring R/I of R by I. We define the operations for a and b in R:

$$(a+I)+(b+I)=(a+b)+I,$$
$$(a+I)(b+I)=ab+I.$$

2.2 The Homomorphism Theorem (3.1)

For a homomorphism φ from R to S, taking $I=\mathrm{Ker}(\varphi)$, we have that $R/I \cong \varphi(R)$, via the map $r+I \mapsto \varphi(r)$.

Proof. We consider the proposed map and name it ψ. We can see that ψ is well defined as for some r in R, for any r' in $r+I$, $r'=r+i$ for some i in I so:

$$\varphi(r')=\varphi(r)+\varphi(i)=\varphi(r).$$

Additionally, ψ is trivially a homomorphism, and is surjective by the definition of the image, so we consider injectivity. If for some r in R, we have $\psi(r+I)=0$ then:

$$\varphi(r)=0 \implies r \in I \implies r+I=I,$$

so ψ is an isomorphism. $\square$

2.3 Chinese Remainder Theorem (3.4)

For positive, coprime integers m and n:

$$\mathbb{Z}/(mn\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

2.4 Properties of the Integers (3.6)

We have the following properties of $\mathbb{Z}$:

- every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer n,
- every ring R admits a unique homomorphism from $\mathbb{Z}$ to R,
- every ring R contains a unique subring which is either isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some non-negative integer n.

2.5 Composition of Ideals (3.8)

For I and J ideals of a ring R:

- $I \cap J$ is an ideal,
- $I + J$ is an ideal,
- $IJ = \{\sum_{k=1}^{n} i_k j_k : n \in \mathbb{N}, (i_k)_{k\in[n]} \in I^n, (j_k)_{k\in[n]} \in J^n\}$ is an ideal.

2.6 Ideals with Units (3.10)

For an ideal I of a ring R, if I contains r in $R^\times$, then $I = R$.

Proof. By definition, we have some s such that $rs = 1$, so 1 is in I as it is an ideal. But then for any x in R, we must have $1 \cdot x$ in I, so $I = R$. □

2.7 Classification of Fields (3.11)

A ring $R \neq \{0\}$ is a field if and only if the only ideals of R are $\{0\}$ and R.

Proof. ($\Longrightarrow$) We have that $R^\times = R \setminus \{0\}$, so every non-zero ideal contains a unit, so must be R by (2.6).

($\Longleftarrow$) For $r \neq 0$ in R, we take $I = \{rx : x \in R\}$ which is a non-zero ideal. By assumption, $I = R$ so 1 is in I, thus $rx = 1$ for some x in R. Thus, r is a unit. □

2.8 Homomorphisms from Fields (3.13)

For a ring homomorphism φ from R to $S \neq \{0\}$, if R is a field, φ is injective.

Proof. The kernel of φ is either R or $\{0\}$ by (2.7), so we consider the cases. If the kernel is R, then $S = \{0\}$, a contradiction, so the kernel must be $\{0\}$. □

2.9 Induced Ideals (3.15)

For a surjective ring homomorphism φ from R to R', with $I \subseteq R$ and $I' \subseteq R'$ ideals, we have that:

1. $\varphi(I)$ is an ideal of R',
2. $\varphi^{-1}(I')$ is an ideal of R containing $\mathrm{Ker}(\varphi)$,
3. there is a bijection from the ideals of R containing $\mathrm{Ker}(\varphi)$ to the ideals of R'.

Proof of (3). We will show that $I = \varphi^{-1}(\varphi(I))$ (the case for $I' = \varphi(\varphi^{-1}(I'))$ is analogous). For x in I, we have that $\varphi(x)$ is in $\varphi(I)$ so x is in $\varphi^{-1}(\varphi(x))$. Thus, $I \subseteq \varphi^{-1}(\varphi(I))$. For x in $\varphi^{-1}(\varphi(x))$, we have that $\varphi(x)$ is in $\varphi(I)$, so $\varphi(x) = \varphi(y)$ for some y in I. As $\varphi(x - y) = 0$, $x - y$ is in $\mathrm{Ker}(\varphi)$ so we have $x = (x - y) + y$ which is in I, as required. $\square$

2.10 The Isomorphism Theorems (3.17)

We take R to be a ring.

2.10.1 The First Isomorphism Theorem

This is the same as the Homomorphism Theorem.

2.10.2 The Second Isomorphism Theorem

For $I \subseteq J \subseteq R$ ideals of R, we have that J/I is an ideal of R/I and:

$$\frac{R/I}{J/I} \cong R/J.$$

2.10.3 The Third Isomorphism Theorem

For a subring S of R, and I an ideal of R, we have that $S + I$ is a subring with $I \subseteq S + I$ and $S \cap I \subseteq S$ ideals and:

$$\frac{S + I}{I} \cong \frac{S}{S \cap I}.$$

3 Integral Domains and Fields

3.1 Integral Domains (4.1)

For a ring R, $a \neq 0$ in R is a zero divisor if for some $b \neq 0$ in R, $ab = 0$. We say R is an integral domain if it has no zero divisors.

3.2 Preservation of Isomorphism

Ring isomorphisms preserve units and zero divisors, so the domain is a field / integral domain if and only if the codomain is a field / integral domain.

3.3 Relating Integral Domains and Fields (4.3)

We have that:

1. all fields are integral domains,
2. R is an integral domain if and only if for all $a \neq 0$ in R, the map $x \mapsto ax$ is injective,
3. every finite integral domain is a field.

Proof. (1) Suppose we have a and b in some field, such that $a \neq 0$ and $ab = 0$. Thus, $a^{-1}ab = 0$, so $b = 0$.

(2) ($\Longleftarrow$) We have that $ax = 0$ if and only if $x = 0$ as R has no zero divisors, so the map is injective by (1.12).
($\Longrightarrow$) We appeal to the contrary and suppose $ax = 0$ for some non-zero a and x in R. As such, the mapping via a has a non-zero kernel, a contradiction by (1.12).

(3) If a integral domain R is finite, then the mapping in (2) is surjective, so for any a in R, there is some x in R such that $ax = 1$. $\square$

3.4 Subrings of Integral Domains (4.4)

Every subring of an integral domain is an integral domain.

3.5 Field of Fractions (4.6)

For an integral domain R, we can consider fractions:

$$\left\{\frac{a}{b} : a \in R, b \in R, b \neq 0\right\},$$

and define an equivalence relation:

$$(a, b) \sim (c, d) \iff ad = bc.$$

with the set of equivalence classes K, forming a field under the ring operations:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

along with the expected additive and multiplicative inverses and identites. This is the field of fractions of R, denoted $f.f.(R)$. We have that R is isomorphic to a subring of K, and if there is an injective homomorphism between two integral domains, there is an induced injection between their respective fields of fractions.

3.6 Maximal Ideals (4.8)

For a ring R, an ideal $I \subset R$ is maximal if there is no ideal J such that $I \subset J \subset R$.

3.7 Prime Ideals (4.9)

For a ring R, an ideal $I \subset R$ is prime if for all ab in I, either a or b is in I.

3.8 Maximal and Prime Ideals and their Quotients (4.12-13)

For a ring R with $I \subset R$ an ideal:

1. I is maximal if and only if R/I is a field,
2. I is prime if and only if R/I is an integral domain.

Thus, every maximal ideal is prime since all fields are integral domains.

Proof. (1) By (2.9), there's a bijection from ideals of R containing I amd ideals of R/I. Thus, the ideals of R/I are 0 and R/I if and only if the ideals of R containing I are I and R, which is true if and only if I is maximal.

(2) We consider a and b in R and consider $\bar{a} = a + I$ and $\bar{b} = b + I$:

$$\begin{aligned} a \in I &\iff \bar{a} = I, \\ b \in I &\iff \bar{b} = I, \\ ab \in I &\iff \bar{a}\bar{b} = I. \end{aligned}$$

Thus, if I is prime and $\bar{a}\bar{b} = I$ then either a or b is in I. Also, if R/I is an integral domain and we have ab in I, then either $\bar{a}$ or $\bar{b}$ is in I so either a or b is in I. $\square$

3.9 Existence of Maximal Ideals (4.16)

Every ring $R \neq \{0\}$ has a maximal ideal.

3.10 Ideals within Maximal Ideals (4.17)

For a ring R, every ideal $I \subset R$ is contained in some maximal ideal.

4 Principal Ideal, Euclidean, and Unique Factorisation Domains

4.1 Noetherian Rings (5.1)

A ring R is Noetherian if every increasing chain of ideals in R is finite.

4.2 Finitely Generated Ideals (5.3)

For a ring R with $I \subseteq R$ an ideal, I is generated by i_1, …, i_n in I for some n in $\mathbb{Z}_{>0}$ if:

$$I = i_1 R + \cdots + i_n R = (i_1, \ldots, i_n).$$

4.3 Finitely Generated Ideals in Noetherian Rings (5.4)

A ring is Noetherian if and only if every ideal of R is finitely generated.

Proof. ($\Longrightarrow$) For an ideal $I \subseteq R$, we consider i_1 in I and take $I_1 = (i_1)$. If $I_1 = I$ then we are done, otherwise we consider i_2 in $I \setminus I_1$ and take $I_2 = (i_1, i_2)$. Following this process, we get $I_1 \subset I_2 \subset \cdots \subset I_n$, for some n in $\mathbb{Z}_{>0}$ as R is Noetherian. Thus, we get a finite generating set $(i_1, \ldots, i_n)$ for I.

($\Longleftarrow$) If we have a chain of ideals $I_1 \subset I_2 \subset \cdots$, then $I = \bigcup_{k \in \mathbb{Z}_{>0}} I_k$ is finitely generated by some $(i_1, \ldots, i_n)$ by assumption. For each k in $[n]$, i_k must be in I_{m_k} for some m_k, so taking $m = \max(m_1, \ldots, m_n)$, $I_m = I$ as required. $\square$

4.4 Preservation of Noetherian Rings (5.5-6)

All quotients of, products of, and polynomials with coefficients in a Noetherian ring are Noetherian rings.

Proof of Quotients. For a Noetherian ring R with I an ideal of R, we consider φ from R to R/I mapping $r \mapsto r + I$. By (2.9), we have a bijection from ideals in R containing I and ideals of R/I via φ which preserves the Noetherian property. $\square$

4.5 Divisibility (5.10-12)

For an integral domain R, we say that b in R divides a in R if there exists c in R such that $a = bc$. Thus, a is in (b) and similarly $(a) \subseteq (b)$. We note that such a c is unique.

If a and b both divide each other ($(a) = (b)$, or $a = b\varepsilon$ for some unit ε in R), we say they are associates. For some $p \neq 0$ in R where p is not a unit, have that:

$$p \text{ irreducible} \iff \big[p = ab \implies a \in R^\times \text{ or } b \in R^\times\big],$$
$$p \text{ prime} \iff \big[p \,|\, ab \implies p \,|\, a \text{ or } p \,|\, b\big] \iff (p) \text{ is a non-zero prime ideal.}$$

4.6 Irreducible Primes (5.14)

For an integral domain R, primes of R are irreducible.

Proof. For a prime p in R with b and c in R such that $p = bc$, so b and c both divide p. By the definition of primes, we have that p divides bc so either p divides b or p divides c. As such, if p divides b then p and b are associate so c is a unit (and similarly for p dividing c). □

4.7 Factorisation (5.16)

For a Noetherian integral domain R, every $r \neq 0$ in R can be factored as:

$$r = \varepsilon q_1 q_2 \cdots q_n,$$

for some unit ε in R and $q_1, \ldots, q_n$ irreducible in R for some n in $\mathbb{Z}_{\geq 0}$.

Proof. If r is a unit, then we are done with $\varepsilon = r$ and $n = 0$. If r is not a unit, we first want to show that $r = q_1 s$ for some irreducible q_1 and s in R.

If r is irreducible, we can take $q_1 = r$ and $s = 1$. If r is not irreducible, then $r = b_1 s_1$ for some non-units b_1 and s_1 in R. We continue, if b_1 is irreducible we are done, otherwise, we write $b_1 = b_2 s_2$ so $r = b_2 s_1 s_2$ for non-units b_2 and s_2. Applying this process repeatedly, until we have $r = b_n s_1 \cdots s_n$ with b_n irreducible. This process terminates as b_{k+1} divides b_k for all k in $[n-1]$ and this implies that:

$$(r) \subset (b_1) \subset (b_2) \subset \cdots, \tag{$*$}$$

which must terminate as R is Noetherian. Using this fact, we can write $r = q_1 r_1$ for some irreducible q_1 and r_1 in R. If r_1 is irreducible we are done, otherwise we apply the process repeatedly, yielding $r = q_1 \cdots q_n r_n$ which terminates by similar reasoning to $(*)$. □

4.8 Unique Factorisation Domains (UFD) (5.17)

For an integral domain R, we say that R is a UFD if every $r \neq 0$ in R is a product of finitely many irreducible elements and a unit of R, unique up to reordering and units.

4.9 Confluence of Primality and Irreducibility (5.23)

For a UFD R, p in R is prime if and only if p is irreducible.

Proof. ($\Longrightarrow$) Proved in (4.6).

($\Longleftarrow$) We know that p is non-zero and not a unit as it is irreducible. We suppose that p divides some ab for a and b in R, so $ab = pc$ for some c in R. Using the properties of UFDs, we factor a, b, and c into irreducibles which, by uniqueness, must contain p (as $ab = pc$). Thus, p divides a or b so p is prime. $\square$

4.10 Highest Common Factor (5.24)

For a UFD R, with a and b non-zero in R, the highest common factor of a and b is the product of the common irreducibles in their unique factorisation (which is well-defined up to units). Taking $h = \mathrm{hcf}(a, b)$:

- h divides a and b,
- $a = hx$ and $a = hy$ for some coprime x and y in R,
- $\mathrm{hcf}(ac, bc) = c \cdot \mathrm{hcf}(a, b)$ for any $c \neq 0$ in R,
- if a and b are coprime and a divides bc for some c in R, then a divides c.

4.11 Coprimaility (5.25)

For a UFD R, with a and b non-zero in R, a and b are coprime if $\mathrm{hcf}(a, b)$ is a unit.

4.12 Principle Ideal Domains (PID) (5.28)

For an integral domain R, we have that R is a principle ideal domain if every ideal of R is principle (generated by a single element).

4.13 Irreducibility, Primality, and Ideal Maximality in PIDs (5.31)

For a PID R, with p non-zero and not a unit in R:

$$p \text{ irreducible} \Longleftrightarrow p \text{ prime} \Longleftrightarrow (p) \text{ prime} \Longleftrightarrow (p) \text{ maximal}.$$

Proof. As R is an integral domain we already have:

$$(p) \text{ maximal} \implies (p) \text{ prime} \iff p \text{ prime} \implies p \text{ irreducible}.$$

So, it is sufficient to show that:

$$p \text{ irreducible} \implies (p) \text{ maximal}.$$

We suppose p is irreducible and $(p) \subseteq I \subseteq R$ for some ideal I. As R is a PID, we know that $I = (a)$ for some a in R so:

$$\begin{aligned} (p) \subseteq (a) &\implies a \text{ divides } p \\ &\implies p = ab \text{ for some } b \in R \\ &\implies a \in R^\times \text{ or } b \in R^\times && (p \text{ irreducible}) \\ &\implies I = R \text{ or } (p) = I, \end{aligned}$$

as required. □

4.14 UFDs from PIDs (5.34)

Every PID is a UFD.

Proof. For a PID R, we know that R is Noetherian by (4.3) so every a can be expressed as a product of irreducible elements in R, say:

$$a = up_1 \cdots p_n,$$

for some unit u and irreducible $p_1, \ldots, p_n$ in R. We suppose there is another factorisation of a:

$$a = vq_1 \cdots q_m,$$

for some unit v and irreducible $q_1, \ldots, q_m$ in R. By (4.13), we know that $p_1, \ldots, p_n, q_1, \ldots, q_m$ are all prime (in particular, they are not units). Thus, if $n = 0$ then $u = a = v$, the factorisation is unique. If $n > 0$ then as p_1 divides a, it must divide q_i for some i in $[m]$. Since q_i is irreducible, $p_1 = q_i$ up to units. Through cancellation (R is an integral domain) and iteration, we see that these factorisations are identical up to reordering. So, R is a UFD. □

4.15 Euclid's Algorithm (5.36)

For a PID R with a and b non-zero in R and c generating the ideal (a, b), we have that $c = \text{hcf}(a, b)$ and $c = ax + by$ for some x and y in R.

Proof. As c generates (a,b), c is in (a,b) so $c = ax + by$ for some x and y. As $(a) \subseteq (a,b)$, $(b) \subseteq (a,b)$ and, $(c) = (a,b)$, c divides both a and b so divides $\mathrm{hcf}(a,b)$ by definition. However, $\mathrm{hcf}(a,b)$ divides both a and b so must divide $ax + by = c$. As such, $c = u \cdot \mathrm{hcf}(a,b)$ for some unit u but since the highest common factor is defined up to units, we can say $c = \mathrm{hcf}(a,b)$. $\square$

4.16 Degree (5.39)

For a field K and a polynomial f in $K[x]$, we say that the largest power of x with a non-zero coefficient is the degree of f, written as $\deg(f)$. We have that $\deg(0) = -\infty$ and for some g in $K[x]$:

$$\begin{aligned} \deg(fg) &= \deg(f) + \deg(g), \\ \deg(f+g) &= \max(\deg(f), \deg(g)). \end{aligned}$$

4.17 Division with Remainder (5.41)

For a field K with f and $g \neq 0$ in $K[x]$, there exists unique q and r in $K[x]$ with $\deg(r) < \deg(g)$ and $f = qg + r$.

Proof. For uniqueness, if $f = q_1 g + r_1 = q_2 g + r_2$ satisfying the conditions in the lemma then $(q_1 - q_2)g = r_1 - r_2$ but $(q_1 - q_2)g$ must have degree at least $\deg(g)$ unless $q_1 = q_2$ and $r_1 - r_2$ has degree strictly less than g by definition so $q_1 = q_2$ and $r_1 = r_2$.

For existence, if $f = a_n x^n + \cdots + a_0$ and $g = b_m x^m + \cdots + b_0$ we suppose $m \leq n$ as otherwise, we can take $q = 0$ and $r = f$. Then, we repeatedly map f as follows:

$$f \mapsto f - \frac{a_n}{b_m} x^{n-m} g,$$

until $\deg(f) < \deg(g)$, r is this result from this iteration, and then $f - r$ is clearly a multiple of g. $\square$

4.18 Polynomials over Fields (5.43)

For a field K, $K[x]$ is a PID.

Proof. For an ideal I of $K[x]$, if $I = \{0\}$ then it is principal. Otherwise, we choose g in $I \setminus \{0\}$ of minimal degree. For any f in I, we write $f = q \cdot g + r$ as in (4.17) and see that $r = f - q \cdot g$ which is in I. Since $\deg(r) < \deg(g)$, it must be that $r = 0$ by the minimality of g so $I = (g)$. $\square$

4.19 Euclidean Domains (5.44, 5.47)

For an integral domain R, R is Euclidean if there is a map δ from $R \setminus \{0\}$ to $\mathbb{Z}_{\geq 0}$ such that for all a and b in $R \setminus \{0\}$:

- there exists q and r such that $a = q \cdot b + r$ and either $r = 0$ or $\delta(r) < \delta(b)$,
- $\delta(a) < \delta(ab)$.

Every Euclidean domain is a PID.

Proof. Similar to that of (4.18). $\square$

4.20 Ring Hierarchy

For the ring definitions we have defined, we can say that:

$$\text{fields} \subseteq \text{Euclidean domains} \subseteq \text{PIDs} \subseteq \text{UFDs} \subseteq \text{integral domains} \subseteq \text{rings}.$$

5 Gauss' Lemma and Polynomial Reducibility

5.1 Content of Polynomials (6.3)

For a UFD R and f a non-zero polynomial in $R[x]$, the highest common factor of the coefficients of f is the content of f denoted by c_f.

5.2 Primitive Polynomials (6.2)

For a UFD R, a polynomial f in $R[x]$ is primitive if $c_f = 1$. Any polynomial f in $R[x]$ can be written as $c_f \cdot f^*$ where f^* is a primitive polynomial in $R[x]$.

5.3 Gauss' Lemma (6.6)

The product of primitive polynomials is primitive.

Proof. For a UFD R, we take f and g primitive in R such that:

$$\begin{aligned} f &= a_n x^n + \cdots + a_1 x + a_0, \\ g &= b_m x^m + \cdots + b_1 x + b_0, \\ fg &= c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \end{aligned}$$

for n and m in $\mathbb{Z}_{\geq 0}$, a_i, b_j, and c_k in R for i in $[n]$, j in $[m]$, and k in $[n+m]$. For any irreducible q in R, q does not divide all of $a_0, \ldots, a_n$ as f is primitive, we take i to be maximal such that q does not divide a_i. Similarly, we take j maximal such that q does not divided b_j. We consider c_{i+j}:

$$c_{i+j} = \underbrace{a_{i+j}b_0 + \cdots + a_{i+1}b_{j-1}}_{\text{all divisible by } q} + a_i b_j + \underbrace{a_{i-1}b_{j+1} + \cdots + a_0 b_{i+j}}_{\text{all divisible by } q}.$$

Since R is a UFD, as q doesn't divide a_i and b_j, q doesn't divide $a_i b_j$ so c_{i+j} is not divisible by q. □

5.4 Content under Multiplication (6.7)

For a field of fractions F of a UFD R, with f and g in $F[x]$, we have that $c_{fg} = c_f c_g$.

Proof. Application of (5.2) and (5.3). □

5.5 Properties of UFDs and their Polynomials (6.8)

For a UFD R:

1. for a unit u in R, u is a unit in $R[x]$,
2. for a prime p in R, p is a prime in $R[x]$,
3. taking F to be the field of fractions of R, for f in $R[x]$ with positive degree, f is prime in $R[x]$ if and only if f is primitive in $R[x]$ and irreducible in $F[x]$.

Proof. (1) If $uv = 1$ for some v in R, the same holds in $R[x]$ as $R \subseteq R[x]$.

(2) Similar to the proof of (5.3), if p doesn't divide f or g in $R[x]$, we show that it doesn't divide fg.

(3) ($\Longleftarrow$) We suppose that for some g and h in $R[x]$, f divides gh. As such, f divides gh in $F[x]$ and since f is irreducible and prime in $F[x]$, we have that f divides g or h. We suppose (without loss of generality) that f divides g so $g = k \cdot f$ for some k in $F[x]$. We write f, g, and k as:

$$f = c_f \cdot f^*, \qquad g = c_g \cdot g^*, \qquad k = c_k \cdot k^*,$$

where c_f is in $R^\times$ as f is primitive, c_g is in R as g is in $R[x]$, c_k is in $F^\times$, and f^*, g^*, and k^* are primitive polynomials in $R[x]$. Since $g = k \cdot f$, we can deduce that:

$$\frac{c_g}{c_f c_k} \cdot g^* = f^* \cdot k^*.$$

We know that $u = \frac{c_g}{c_f c_k}$ is in $R^\times$ as $f^* \cdot k^*$ must be primitive and contents are unique up to units, so we write:

$$g = \frac{c_g}{u c_f} \cdot k^* \cdot f.$$

Since c_g is in R and uc_f is in $R^\times$, f divides g in $R[x]$ as required.

($\Longrightarrow$) By contrapositive, we first consider if f is not primitive, in which case $f = c_f \cdot f^*$ where f^* is primitive in $R[x]$ is a non-trivial factorisation of f in $R[x]$ so f is not irreducible, and thus, not prime. If f is reducible in $F[x]$, $f = gh$ for some non-constant g and h in $F[x]$. Then, as in the previous direction, $f = c_f g^* h^*$ is reducible in $R[x]$ so f is not prime. $\square$

5.6 UFDs and their Polynomials (6.10)

For a UFD R, $R[x]$ is a UFD. Furthermore, the primes of $R[x]$ are the primes of R and primitive irreducible polynomials of positive degree, and $R[x]^\times = R^\times$. We can recursively apply this, so $R[x_1, \dots, x_n]$ is a UFD for any n in $\mathbb{Z}_{\geq 0}$.

Proof. (**Units**) By (5.5(1)), $R^\times \subseteq R[x]^\times$, so we consider f in $R[x]^\times$. As such, there's some g in $R[x]$ with $fg = 1$. Thus:

$$\deg(f) + \deg(g) = \deg(fg) = 1,$$

so f and g must be constant polynomials, meaning they are in R. Hence, f is in $R^\times$ so $R[x]^\times = R^\times$.

(**Primes**) By (5.5(2)), we know the primes of R are in $R[x]$. Also, by (5.5(3)), we know that primitive irreducible polynomials of positive degree are prime.

(**Factorisation**) For f non-zero in $R[x]$, with F the field of fractions of R, since $F[x]$ is a UFD (as it is a field) we can write:

$$f = c \cdot f_1 \cdots f_n,$$

for c in $F^\times$, n in $\mathbb{Z}_{\geq 0}$, and $f_1, \dots, f_n$ irreducible in $F[x]$. We then write:

$$\begin{aligned} c^* &= c \cdot c_{f_1} \cdots c_{f_n} \in F^\times, \\ f &= c^* \cdot f_1^* \cdots f_n^*. \end{aligned}$$

But, $c^* = c_f$ as $f_1^* \cdots f_n^*$ is primitive by Gauss' Lemma, so is in R. As such, we can write $c^* = u \cdot q_1 \cdots q_m$ for u in $R^\times$, m in $\mathbb{Z}_{\geq 0}$, and $q_1, \dots, q_n$ prime in $F[x]$. Thus, we can write:

$$f = u \cdot \underbrace{q_1 \cdots q_m \cdot f_1^* \cdots f_n^*}_{\text{prime in } R[x]}.$$

As in the proof of (4.14), since we showed that every f in $R[x]$ can be factored into primes, not just irreducibles, the factorisation is automatically unique. $\square$

5.7 Eisenstein's Criterion (7.1)

For a UFD R, f primitive in $R[x]$ with positive degree so $f = a_n x_n + \cdots + a_0$ for some n in $\mathbb{Z}_{>0}$ and $a_n, \ldots, a_0$ in R. If there is a prime p in R such that:

- p doesn't divide a_n,
- p divides $a_0, \ldots, a_{n-1}$,
- p^2 doesn't divide a_0,

then f is irreducible in $R[x]$ and also $F[x]$ where F is the field of fractions of R. Polynomials satisfying this criterion are called Eisenstein polynomials (at p).

Proof. We suppose $f = gh$ where g and h are in $R[x]$ and have positive degree. We take:

$$\begin{aligned} g &= b_m x^m + \cdots + b_0, \\ h &= c_{n-m} x^{n-m} + \cdots + c_0, \end{aligned}$$

for some m in $\mathbb{Z}_{>0}$ and $b_0, \ldots, b_m, c_0, \ldots, c_{n-m}$ in R. We know that p doesn't divide $a_n = b_m c_{n-m}$, so p doesn't divide b_m or c_{n-m}. We take i to be minimal such that p doesn't divide b_i, and j to be minimal such that p doesn't divide c_j. This implies that p doesn't divide a_{i+j} so $i + j = n$, thus $i = m$ and $j = n - m$. As such, p divides b_0 and c_0 so p^2 divides a_0, a contradiction. □

5.8 Irreducibility and Linear Substitution (7.5)

For a field K with f in $K[x]$, a and b in K with $a \neq 0$ then $f(x)$ is irreducible if and only if $f(ax + b)$ is irreducible.

5.9 Roots and Divisibility (7.8)

For a field K with f in $K[x]$ and α in K:

$$f(\alpha) = 0 \iff x - \alpha \text{ divides } f(x).$$

Proof. ($\Longrightarrow$) We divide $f(x)$ with remainder by $(x - \alpha)$ so $f(x) = g(x)(x - \alpha) + r$ for some g in $K[x]$ and r in K (since $\deg(r) < \deg(x - \alpha) = 1$). So, we have $f(\alpha) = g(\alpha)(x - \alpha) + r = r = 0$, thus $f(x) = g(x)(x - \alpha)$ as required.

($\Longleftarrow$) We have $f(x) = g(x)(x - a)$ for some g in $K[x]$, so $f(\alpha) = 0$. □

5.10 The Second Criterion (7.9)

For a field K with f in $K[x]$ with degree equal to 2 or 3:

$$f \text{ is irreducible} \iff f \text{ has no roots in } K.$$

Proof. We consider the following equivalences:

$$\begin{aligned} f \text{ reducible} &\iff f \text{ has a factor of degree 1} \\ &\iff ax + b \text{ divides } f(x) \text{ for some } a \neq 0 \text{ and } b \text{ in } K \\ &\iff x + \frac{b}{a} \text{ divides } f(x) \\ &\iff f\left(-\frac{b}{a}\right) = 0, \end{aligned} \tag{5.9}$$

as required. $\square$

5.11 Finding Roots (7.10)

For a UFD R with K its field of fractions, we consider f in $R[x]$ with degree $n \geq 0$ and coefficients $a_n, \ldots, a_0$ in R. For some α in K, written in its simplest form as $\alpha = \frac{r}{s}$ ($\text{hcf}(r, s) = 1$), if $f(\alpha) = 0$ then r divides a_0 and s divides a_n.

Proof. By (5.9), we know that $x - \alpha$ divides f in $K[x]$ so $sx - r$ divides f^* in $K[x]$ since f^* is the same as f up to units in K. We note that $sx - r$ is primitive since $\text{hcf}(r, s) = 1$ and irreducible as it has degree 1. As such, $sx - r$ is prime in $R[x]$. From an **exercise** (see (5.6)), we deduce that $sx - r$ divides f^* in $R[x]$ also.

So, $f = c_f(sx - r)g$ for some polynomial g in $R[x]$ of degree $n - 1$ with coefficients $b_{n-1}, \ldots, b_0$ in R. This implies that $a_0 = -c_f r b_0$ is divisible by r and $a_n = c_f s b_{n-1}$ is divisible by s. $\square$

5.12 Monic Polynomials (7.14)

A polynomial is monic if its leading coefficient is 1.

5.13 Reflected Irreducibility from Monic Images on Induced Maps (7.15)

For a ring homomorphism on integral domains φ from R to S with φ also acting as the induced map on $R[x]$ to $S[x]$, we have that if f in $R[x]$ is monic and $\varphi(f)$ is irreducible then f is irreducible.

Proof. We suppose that f is reducible so $f = gh$ for some g and h in $R[x]$ with degrees m and k and coefficients $b_m, \ldots, b_0$ and $c_k, \ldots, c_0$ respectively. As f is monic, we have $b_m c_k = 1$ so we can simply rewrite $g \mapsto \frac{1}{b_m} g$ and $h \mapsto \frac{1}{c_k}$, so we will just assume g and h are monic, $b_m = c_k = 1$, without loss of generality. As such:

$$f(x) = (x^m + b_{m-1}x^{m-1} + \cdots + b_0)(x^k + c_{k-1}x^{k-1} + \cdots + c_0).$$

We have m and k strictly greater than zero as otherwise our factorisation $f = gh$ was not proper, so:

$$\varphi(f) = (x^m + \varphi(b_{m-1})x^{m-1} + \cdots + \varphi(b_0))(x^k + \varphi(c_{k-1})x^{k-1} + \cdots + \varphi(c_0)),$$

is a proper factorisation of $\varphi(f)$, a contradiction. □

5.14 The Third Criterion (7.18)

For an integral domain R with f in $R[x]$ monic, if f mod (p) is irreducible for some prime ideal (p) in R, f is irreducible.

Proof. By (5.13) on the quotient homomorphism. □

5.15 Irreducibility in the Rationals (7.21)

For f in $\mathbb{Z}[x]$ with leading coefficient α, p prime in $\mathbb{Z}$, if $\alpha \not\equiv 0 \bmod p$ and f mod (p) is irreducible then f is irreducible in $\mathbb{Q}[x]$.

Proof. Similar to (5.14). □

6 Field Extensions

6.1 Polynomials in Extended Fields (7.24)

For rings R and S with $R \subseteq S$ and f in $R[x]$, we refer to the image of f in $S[x]$ as 'f over S'.

6.2 Finite Fields and Integers Modulo Primes (8.2)

For a prime p in $\mathbb{Z}$, we have that the finite field of size p, denoted by $\mathbb{F}_p$, is $\mathbb{Z}/p\mathbb{Z}$.

6.3 The Field of Rational Functions (8.3)

We define the field of rational functions over R as the field of fractions of $R[x]$.

6.4 Subfields and Extensions (8.5, 8.19)

For fields K and L with $K \subseteq L$, we say that K is a subfield of L and L is an extension of K, which may be denoted by L/K.

6.5 Conditions for Subfields (8.9)

For a field K with $U \subseteq K$, U is a subfield if and only if:

- $\{0, 1\} \subseteq U$,
- U is closed under addition and additive inverses,
- U is closed under multiplication and multiplicative inverses.

Proof. Follows from (1.5). □

6.6 Prime Subfields (8.11)

For a field K, K either contains $\mathbb{F}_p$ for some unique prime p in $\mathbb{Z}$ or $\mathbb{Q}$. This is the prime subfield of K.

Proof. By (2.4), there is a unique homomorphism from $\mathbb{Z}$ to K so:

$$\mathbb{Z}/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) \subseteq K.$$

As K is a field, $\operatorname{Im}(\varphi)$ must be an integral domain so $\operatorname{Ker}(\varphi)$ is a prime ideal. As such, $\operatorname{Ker}(\varphi)$ is either $\{0\}$ or $\mathbb{F}_p$ for some prime p in $\mathbb{Z}$. In the former case, $\mathbb{Z}$ is a subring of K so its field of fractions $\mathbb{Q}$ is a subfield of K. In the latter case, $\mathbb{F}_p$ is a subfield of K. By the uniqueness of φ, such a subfield is unique. □

6.7 The Field Characteristic (8.12)

We define the characteristic function on fields:

$$\operatorname{char}(K) = \begin{cases} 0 & \text{if } \mathbb{Q} \subseteq K \\ p & \text{if } \mathbb{F}_p \subseteq K. \end{cases}$$

6.8 Vector Spaces (8.15)

For fields K and L with $K \subseteq L$, L is a vector space over K.

Proof. Follows from the field axioms. □

6.9 Degree of Field Extensions (8.20)

For a field extension L/K, the degree of the extension is:

$$[L : K] = \dim(L \text{ as a } K\text{-vector space}).$$