Sketch Notes — Rings and Fields

Neil Donaldson

Fall 2018

Text

- *An Introduction to Abstract Algebra*, John Fraleigh, 7th Ed 2003, Adison–Wesley (optional).

Brief reminder of groups

You should be familiar with the majority of what follows though there is a lot of time to remind yourself of the harder material! Try to complete the proofs of any results yourself.

Definition. A *binary structure* $(G, \cdot)$ is a set G together with a function $\cdot : G \times G \to G$. We say that G is *closed* under $\cdot$ and typically write $\cdot$ as juxtaposition.[1]

A *semigroup* is an *associative* binary structure:

$$\forall x, y, z \in G,\ x(yz) = (xy)z$$

A *monoid* is a semigroup with an *identity element*:

$$\exists e \in G \text{ such that } \forall x \in G,\ ex = xe = x$$

A *group* is a monoid in which every element has an *inverse*:

$$\forall x \in G,\ \exists x^{-1} \in G \text{ such that } xx^{-1} = x^{-1}x = e$$

A binary structure is *commutative* if $\forall x, y \in G$, $xy = yx$. A group with a commutative structure is termed *abelian.*

A *subgroup*[2] is a non-empty subset $H \subseteq G$ which remains a group *under the same binary operation.* We write $H \leq G$.

Lemma. *H is a subgroup of G if and only if it is a non-empty subset of G closed under multiplication and inverses in G.*

Standard examples of groups: sets of numbers under addition ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, n\mathbb{Z}$, etc.), matrix groups.

Standard families: cyclic, symmetric, alternating, dihedral.

[1] You should be comfortable with both multiplicative and additive notation.

[2] More generally any substructure.

Cosets and Factor Groups

Definition. If $H \leq G$ and $g \in G$, then the *left coset of H containing G* is the set

$$gH = \{gh : h \in H\}$$

Clearly $k \in gH \iff \exists h \in H$ such that $k = gh \iff k^{-1}g \in H$.

The right coset Hg is defined similarly.

A subgroup H of G is *normal* (written $H \triangleleft G$) if $gH = Hg$ for all $g \in G$.

Lemma. *$H \triangleleft G \iff \forall g \in G, h \in H$ we have $ghg^{-1} \in H$*

Theorem. *The set of (left) cosets of $H \triangleleft G$ has a natural group structure defined by $g_1H \cdot g_2H := (g_1g_2)H$. We call this the* factor group ${}^{G}\!/_{H}$.

Definition. For each $n \in \mathbb{N}$, we define $\mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

Homomorphisms

Definition. A function $\phi : (G, \cdot) \to (H, \star)$ of binary structures is a *homomorphism* if

$$\forall x, y \in G, \quad \phi(x \cdot y) = \phi(x) \star \phi(y)$$

An *isomorphism* is a bijective homomorphism: we write $G \cong H$ if there exists an isomorphism from G to H.
If ϕ is a homomorphism of groups, then its *kernel* and *image* are the sets

$$\ker \phi = \{g \in G : \phi(g) = e\} \qquad \operatorname{Im} \phi = \{\phi(g) : g \in G\}$$

Lemma. $\ker \phi \triangleleft G$.

Theorem (1st isomorphism theorem)**.**

1. *If $\phi : G \to H$ is a homomorphism, then ${}^{G}\!/_{\ker \phi} \cong \operatorname{Im} \phi$ via the isomorphism*

$$\mu(gH) := \phi(g)$$

2. *If $H \triangleleft G$ then $\gamma : G \to {}^{G}\!/_{H}$ defined by $\gamma(g) = gH$ is a homomorphism, whence* every *factor group appears as in part 1.*

Example Let $\zeta = e^{\frac{2\pi i}{9}}$ and define

$$\phi : \mathbb{Z} \to \mathbb{C} : x \mapsto \zeta^x$$

This is a homomorphism with kernel $\ker \phi = 9\mathbb{Z}$: the 1st isomorphism theorem reads

$${}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \cong \operatorname{Im} \phi = \{1, \zeta, \zeta^2, \ldots, \zeta^8\}$$

which is the multiplicative group of 9th roots of unity.

18 Rings and Fields

Definition 18.1. A *ring* is a set R with two binary operations $+$ and $\cdot$ (always called addition and multiplication) for which:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is a semigroup (R is closed under $\cdot$ and $\cdot$ is associative).
3. The *left* and *right distributive laws hold*:

$$\forall x, y, z \in R,\ x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{and} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

A ring is simply an abelian group (axiom 1) with a bit of extra structure that making it behave similarly to the integers: we have a notion of multiplication (axiom 2) which interacts with addition (axiom 3) in the expected way. Rings often *feel* easier than groups because they behave so similarly to the familiar integers.

Definition 18.2. A ring $(R, +, \cdot)$ is *commutative* if $\cdot$ is commutative.

Simple Examples

- Sets of numbers: $\mathbb{Z}$, $n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual addition and multiplication. These are all commutative rings.
- The set of polynomials $R[x]$ whose coefficients lie in some ring R. The addition and multiplication are inherited from that of R. For instance, if $R = \mathbb{Z}$, then

  $$(1 + 3x^2)(2x - 4x^2) = 2x - 4x^2 + 6x^3 - 12x^4$$

  $R[x]$ will be commutative precisely when R is commutative. More generally, the set of functions $f : R \to R$ also forms a ring using the addition and multiplication of elements in R.
- The set $M_n(R)$ of $n \times n$ matrices whose entries lie in a ring R. Typically $M_n(R)$ is a non-commutative ring, regardless of whether R is commutative.
- The *quaternions* are the set

  $$\mathcal{Q} = \{w + ix + jy + kz : w, x, y, z \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,\ ij = k \text{ etc.}\}$$

  Think of this like a copy of $\mathbb{R}^4$ with basis $\{1, i, j, k\}$. Addition is the usual addition in $\mathbb{R}^4$. Multiplication works as with the complex numbers: i, j and k act like three different copies of the imaginary unit i. Finally, distinct elements i, j, k multiply following the right-hand rule for cross-products:

  $$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik$$

  It is a little work to check that $(\mathcal{Q}, \cdot)$ is associative. Since, e.g., $ij = -ji$, we have a non-commutative ring.

- The *factor rings* $\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}}$ are defined in the same manner as for groups: we will do this more formally later. It is perfectly acceptable to write

  $$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

  as long as you appreciate that the symbol x refers to the equivalence class of integers

  $$[x] = \{x + \lambda n : \lambda \in \mathbb{Z}\}$$

- A *direct product* of rings $R_1 \times \cdots \times R_k$ is defined exactly as for groups. For example, in the ring $\mathbb{Z} \times M_2(\mathbb{R})$ we could write

  $$\left(2, \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}\right) \cdot \left(-3, \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\right) = \left(-6, \begin{pmatrix} 2 & -3 \\ 3 & -4 \end{pmatrix}\right)$$

Non-examples of rings

- The natural numbers $\mathbb{N}$ do not form an abelian group under addition.
- $M_{m\times n}(R)$ (if $n \neq m$): multiplication is not well-defined.
- General vector spaces are not rings: there is no natural sense of product! You might suspect that $(\mathbb{R}^3, +, \times)$ is a ring, where $\times$ is the cross-product. However, observe that

  $$\mathbf{i} \times (\mathbf{i} \times \mathbf{j}) = \mathbf{i} \times \mathbf{k} = -\mathbf{j} \neq \mathbf{0} = (\mathbf{i} \times \mathbf{i}) \times \mathbf{j}$$

  The product is not associative! Non-associative algebras are extremely important (Lie Algebras rule parts geometry and of Physics) but they are *not* rings.

Conventions

We've already started following some of these as the conventions are similar to those you are used to following from group theory.

- We will usually just say 'the ring R,' rather than $(R, +, \cdot)$, unless the operations are not clear.
- You should assume that R is a ring unless otherwise stated: e.g. $\mathbb{Z}$, $\mathbb{Z}_n$, etc., are always *rings* in this course. If we need to refer to the *additive group of a ring*, we will write $(R, +)$.
- Since $(R, +)$ is an abelian group, it is typical to denote the *additive identity* by 0. Thus,[3]

  $$\forall x \in R,\ 0 + x = x$$

  We similarly denote *additive inverses* using negatives:

  $$\forall x \in R,\ x + (-x) = 0$$

[3] We only need one side of the identity axiom: $x + 0 = x$ is superfluous since $+$ is commutative.

- Use juxtaposition and exponentiation notation for multiplication unless in the dot is helpful: thus

  $$x \cdot x \cdot x = xxx = x^3$$

- If n is a positive integer and $x \in R$, we will write

  $$n \cdot x = \underbrace{x + \cdots + x}_{n \text{ times}}$$

  This requires a little care: if R is any ring and $x \in R$, we can always write, for instance

  $$3 \cdot x = x + x + x$$

  In the special case where $3 \in R$ (say if $R = \mathbb{Z}$), then $3 \cdot x = 3x$ since we really can multiply 3 by x within R. In general, however, this makes no sense: for example $3x$ is meaningless within the ring $2\mathbb{Z}$ of even integers, since $3 \notin 2\mathbb{Z}$.

Basic Results The basic theorems regarding groups necessarily hold: we state these without proof.

Lemma 18.3. *If $(R, +, \cdot)$ is a ring, then the additive identity 0 and additive inverses are unique. Moreover, the left- and right-cancellation laws hold:*

$$x + y = x + z \implies y = z, \quad \textit{and} \quad x + z = y + z \implies x = y$$

The first genuine results concerning rings involve the interaction of the additive identity with multiplication: essentially this first theorem tells us that 0 and negative signs behave exactly as we expect.

Theorem 18.4 (Laws of Signs)**.** *Let R be a ring:*

1. $\forall x \in R,\ 0x = x0 = 0$
2. $\forall x, y \in R,\ x(-y) = (-x)y = -xy$
3. $\forall x, y \in R,\ (-x)(-y) = xy$

Proof.

1. Since $(R, +)$ is an additive group, we have $0 = 0 + 0$. Multiplying on the right by x and applying a distributive law yields

   $$0x = (0 + 0)x = 0x + 0x$$

   Cancelling $0x$ from both sides (Lemma 18.3) gives half the result; the remainder follows symmetrically.

2. Apply the distributive law to compute

   $$(xy) + (-x)y = (x + (-x))y = 0y = 0 \implies -(xy) = (-x)y$$

   The other version of this is similar.

3. Finally, we apply the first and second results repeatedly:

   $$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$$

■

Further multiplicative structure

Most commonly, we will consider rings where multiplication has more than simple associativity.

Definition 18.5. A ring R is a *ring with 1*, or a *ring with unity*, if $(R, \cdot)$ is a *monoid* (an associative binary structure with an identity). In such a case the[4] *unity*, or *multiplicative identity*, is abstractly denoted 1.

If R is a ring with unity $1 \neq 0$, then an element $x \in R$ is a *unit* if it has a multiplicative inverse:

$$x \text{ a unit} \iff \exists x^{-1} \in R \text{ such that } xx^{-1} = x^{-1}x = 1$$

A ring with unity $1 \neq 0$ is a *division ring* or *skew field* is a ring with unity in which every non-zero element is a unit.
A *field* is a commutative division ring.

To a great many authors 'ring' means 'ring with unity $1 \neq 0$:' this assumption is made so often that it is easy to miss and guarantees that the ring has at least two elements. It is common to refer to a ring *without* unity as a *rng* (no i!), a *pseudo-ring* or a *non-unital ring* if clarity is required. For our purposes, a ring may or may not have a unity: when it does, we will make the standard assumption that $1 \neq 0$.

Examples

- $\mathbb{Z}$ is a commutative ring with unity. The only units are ± 1.
- $n\mathbb{Z}$ has no identity if $n \geq 2$ and thus no units.
- $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields.
- If R is a ring with unity, then so is $R[x]$: the multiplicative identity is the constant polynomial 1. The set of functions $\{f : R \to R\}$ behaves similarly.
- $M_n(R)$ is a ring with unity if R is such: the *identity matrix* is exactly as you expect.
- The quaternions form a *non-commutative division ring*. To see this, note that we can define a *modulus* exactly as with complex numbers:

  $$|q|^2 := q\overline{q} = (w + ix + jy + kz)(w - ix - jy - kz) = w^2 + x^2 + y^2 + z^2$$

  Clearly $|q| = 0 \iff q = 0$, and $q^{-1} = \frac{\overline{q}}{|q|^2}$.

It is worth recalling some elementary number theory for our next result:

Theorem 18.6. *$x \in \mathbb{Z}_n$ is a unit if and only if* $\gcd(x, n) = 1$. *Thus $\mathbb{Z}_n$ is a field if and only if n is* prime.

Proof. Recall Bézout's identity:

$$\gcd(x, n) = 1 \iff \exists \lambda, \mu \in \mathbb{Z} \text{ such that } \lambda x + \mu n = 1$$

It should be clear that λ is an inverse to x in $\mathbb{Z}_n$. ∎

[4] The definite article is appropriate here. The proof that the identity is unique in a group only requires closure, thus a ring with unity has *only one* unity! Explicitly, if 1 and $\hat{1}$ are unities, then $1 \cdot \hat{1}$ must both be 1 and $\hat{1}$...

Theorem 18.7. *If R is a ring with unity, then the set of units $U \subseteq R$ forms a* group under multiplication.

Proof. If $u, v \in U$, quickly check that $v^{-1}u^{-1}$ is an inverse of uv, whence U is closed under multiplication. The associativity, identity and inverse axioms are essentially trivial. ∎

The set of units is often denoted $R^\times$: for example,

$$\mathbb{Z}_{10}^\times = \{1,3,7,9\}$$

Notice that 3 is a generator of this group ($\langle 3 \rangle = \{3,9,7,1\}$) and so $\mathbb{Z}_{10}^\times \cong \mathbb{Z}_4$ is cyclic.[5]

Homomorphisms and Isomorphisms

At first glance these work exactly as for groups. The first novelty is that they must preserve *both* binary structures:

Definition 18.8. Let R, S be rings. A function $\phi : R \to S$ is a homomorphism if

$$\forall x, y \in R, \begin{cases} \phi(x+y) = \phi(x) + \phi(y) \\ \phi(xy) = \phi(x)\phi(y) \end{cases}$$

Additionally, ϕ is an *isomorphism* if it is bijective. We write $R \cong S$ exactly as with isomorphic groups. It should be clear that $\phi : (R,+) \to (S,+)$ is automatically a homo/isomorphism of *groups.*

One delicacy[6] is that, if *both* R, S are rings with unity, then it is common to additionally assume $\phi(1_R) = 1_S$. This is *not guaranteed*! For example,

$$\phi : \mathbb{Z} \to \mathbb{Z} : x \mapsto 0$$

is a homomorphism, although it is extremely boring. Indeed, suppose that $\psi : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism and compute

$$\psi(1) = \psi(1 \cdot 1) = (\psi(1))^2 \implies \psi(1) = 0 \text{ or } 1$$

Since we also require

$$\forall x \in \mathbb{Z}^+,\ \psi(x) = \psi(1 + 1 + \cdots + 1) = \psi(1) + \cdots + \psi(1) = x \cdot \psi(1)$$

and similarly for negative numbers, it follows that the *only* ring homomorphisms $\psi : \mathbb{Z} \to \mathbb{Z}$ are

$$\psi(x) = 0 \text{ or } \psi(x) = x$$

This is much more restrictive that with groups.[7] Some of this discussion is worth generalizing:

Theorem 18.9. *Suppose $\phi : R \to S$ is a homomorphism and R is a ring with unity. If $n \in \mathbb{Z}$, then*

$$\phi(n) = n \cdot \phi(1)$$

In the general context when R does not contain integers, $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$.

---

[5] In number theory, the generator 3 is called a *primitive root* modulo 10. Not all n have primitive roots: indeed the group of units is rarely cyclic.

[6] See the comment on non-unital rings on the previous page.

[7] Recall that $\phi(x) = kx$ defines a *group* homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ for any $k \in \mathbb{Z}$.

Proof. If $n = 0$, this is simply the group theoretic result that $\phi(0_R) = 0_S$: recall,

$$\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R) \implies \phi(0_R) = 0_S$$

by cancellation. When $n \geq 1$ this is simple induction on n. Finally, when $n \leq -1$ the fact that $\phi(-n) = -\phi(n)$ (basic group theory again) finishes things off. ∎

We are now in a position to extend our discussion of direct products of finite cyclic groups.

Corollary 18.10. $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \iff \gcd(m,n) = 1$

Proof. Note that the result is already true for *additive groups*,[8] where we observed that $(1,1)$ is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$ whenever $\gcd(m,n) = 1$. This corresponds to the function

$$\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n : x \mapsto (x,x)$$

being an *isomorphism*. It remains only to see that ϕ is also an isomorphism of *rings*. But this is trivial:

$$\phi(xy) = (xy, xy) = (x,x) \cdot (y,y) = \phi(x) \cdot \phi(y)$$

∎

Example Find all isomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$.
Let $\phi(1) = (a,b)$: since ϕ is to be a homomorphism of additive groups, we see that

$$\phi(x) = x \cdot \phi(1) = (ax, bx)$$

To be an additive isomorphism, we need the order of (a,b) to be 12, whence $\gcd(a,3) = 1 = \gcd(b,4)$. There are *four* group isomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$, corresponding to the generators

$$(a,b) = (1,1), (1,3), (2,1), (2,3)$$

To be a ring homomorphism, we also require

$$\phi(xy) = (axy, bxy) = (a^2xy, b^2xy) = (ax, bx) \cdot (ay, by) = \phi(x) \cdot \phi(y)$$

for *all* x, y. This clearly requires $a^2 \equiv a \mod 3$ and $b^2 \equiv b \mod 4$. Of the above choices, only $(a,b) = (1,1)$ works. There is therefore exactly *one* ring isomorphism.

The above can be generalized: Suppose that $\gcd(m,n) = 1$ so that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

- Every *group isomorphism* $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ has the form $\phi(x) = (ax, bx)$ where $\gcd(a,m) = 1 = \gcd(b,n)$, so that $a \in \mathbb{Z}_m^\times$ and $b \in \mathbb{Z}_n^\times$ are both units.

[8]It also follows from the previous result. If $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a homomorphism, then $\phi(x) = x \cdot \phi(1)$. Letting $\phi(1) = (a,b)$, we see that $\phi(x) = (ax, bx)$. However

$$(0,0) = \phi(x) = (ax, bx) \iff \begin{cases} ax \equiv 0 \mod m \\ bx \equiv 0 \mod n \end{cases}$$

ϕ is surjective only if $x = mn$ is the *smallest* positive integer satisfying the above. But this is if and only if $\gcd(a,m) = 1 = \gcd(b,n) = \gcd(m,n)$.

- Every *ring isomorphism* must be a group isomorphism and additionally satisfy

$$a^2 \equiv a \mod m \quad \text{and} \quad b^2 \equiv b \mod n$$

  Since a, b are already units, it follows that the *only* possibility is to have $a = 1$ and $b = 1$. There is *always only one isomorphism*!

Indeed this is a special case of a useful theorem.

Theorem 18.11. *Having a unity is a structural property. Specifically, suppose that $\phi : R \to S$ is a ring isomorphism (or merely a surjective ring homomorphism) and that R is a ring with unity. Then S is a ring with unity and $1_S = \phi(1_R)$.*

Proof. For all $x \in R$, we have

$$\phi(x) = \phi(1_R x) = \phi(1_R)\phi(x)$$

and similarly $\phi(x) = \phi(x)\phi(1_R)$. Since ϕ is surjective, it follows that $\phi(1_R)y = y = y\phi(1_R)$ for all $y \in S$. ∎

In particular, if $\phi : R \to S$ is a surjective homomorphism where the *group* $(R, +)$ is cyclic, then $\phi(x) = x \cdot 1_S$. In our previous example, we are forced to take $\phi(1) = (1, 1)$ (the unity in $\mathbb{Z}_m \times \mathbb{Z}_n$), whence $\phi(x) = (x, x)$.

Subrings

Just as with groups, we can define substructures.

Definition. Let $(R, +, \cdot)$ be a ring. A subset S is a *subring* of R if $(S, +, \cdot)$ is a ring. We have a similar notion for *subfield.*

Since every subring of R is necessarily a subgroup of $(R, +)$, we can start hunting for subrings by first considering subgroups.

Examples

1. Subrings of $\mathbb{Z}$. Every subgroup has the form $n\mathbb{Z}$ for some $n \in \mathbb{N}_0$. Since the set of multiples of n is closed under multiplication, these are also subrings.
   In contrast to group theory, note that $\mathbb{Z} \not\cong n\mathbb{Z}$ when $n \neq 1$. If we had an isomorphism, $\phi : \mathbb{Z} \to n\mathbb{Z}$ then it must also be an isomorphism of groups, whence $\phi(1)$ would have to be a generator: the only options are $\phi(1) = \pm n \implies \phi(x) = \pm nx$. But for this to be a ring isomorphism, we'd need

$$\forall x, y \in \mathbb{Z},\ \phi(xy) = \phi(x)\phi(y) \implies \pm nxy = nxny$$

   a contradiction.

2. A similar game can be played in $\mathbb{Z}_n$. Every subgroup of $(\mathbb{Z}_n, +)$ has the form $\langle d \rangle = \{kd : k \in \mathbb{Z}\}$ where $d \mid n$. Since $(kd)(ld)$ is still a multiple of d, the subset $\langle d \rangle$ is closed under multiplication and is thus a subring. The subrings of $\mathbb{Z}_n$ are therefore precisely the subgroups of $\mathbb{Z}_n$.

3. Warning! In general, not all subgroups of $(R,+)$ are going to be *subrings* of R. Take, for example, $\langle(1,2)\rangle \leq \mathbb{Z}\times\mathbb{Z}$ as the cyclic subgroup generated by $(1,2)$. This is not a subring of $\mathbb{Z}\times\mathbb{Z}$ since it is not closed under multiplication:

$$(1,2)\cdot(1,2) = (1,4) \notin \langle(1,2)\rangle$$

19 Integral Domains

The ability to factorize is of crucial importance in mathematics. For instance,

$$x^2 = x \iff x^2 - x = 0 \iff x(x-1) = 0 \iff x = 0,\text{ or } 1 \tag{$*$}$$

This calculation should feel completely natural, but is it *always* legitimate? Certainly we feel confident if x is restricted to the real or complex numbers. What about if $x \in \mathbb{Z}_n$ for some n? We can easily find all the solutions to $x^2 \equiv x \mod n$ for all small n by inspection: here is what we find.

n	solutions x to $x^2 \equiv x$
2	$0,1$
3	$0,1$
4	$0,1$
5	$0,1$
6	$0,1,3,4$
7	$0,1$
8	$0,1$
9	$0,1$
10	$0,1,5,6$

While the solutions are usually as expected, when $n = 6$ or 10 we have extras! Indeed the extra solutions correspond to alternative factorizations: for example

$$(x-5)(x-6) \equiv x^2 - 11x + 30 \equiv x^2 - x \mod 10$$

With a little thinking, it should become clear that we will never have this problem of multiple factorizations when n is a *prime*:[9] consider

$$x(x-1) \equiv 0 \mod p \iff p \mid x(x-1) \iff p \mid x \text{ or } p \mid x-1 \iff x \equiv 0,1 \mod p$$

This is because it is impossible to have non-zero remainders multiplying to give 0. We make a general definition.

Definition 19.1. If $a,b \in R$ are non-zero elements for which $ab = 0$, we say that a,b are *zero-divisors.*

For example, $2\cdot 5 = 0 \in \mathbb{Z}_{10}$, $\quad 2\cdot 3 = 0 \in \mathbb{Z}_6$, $\quad \begin{pmatrix}1&1\\3&3\end{pmatrix}\begin{pmatrix}1&-2\\-1&2\end{pmatrix} = 0 \in M_2(\mathbb{R})$.

Definition 19.2. An *integral domain* is a commutative ring with unity which has no zero-divisors.

The most obvious example of an integral domain is the integers themselves! Clearly $ab = 0 \implies a = 0$ or $b = 0$. This is true for any of the standard rings of numbers: $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$. Indeed:

[9] Recall that $p \in \mathbb{N}_{\geq 2}$ is *prime* if $p \mid ab \implies p \mid a$ or $p \mid b$.

Theorem 19.3. *Every field is an integral domain.*

Proof. Every field is a commutative ring with unity. Moreover, if a is a zero-divisor, then it is a non-zero element and thus a unit. Clearly

$$ab = 0 \implies b = 0$$

after multiplying by a^{-1} on the left (this is precisely th argument (†) above. But then a is not a zero-divisor! ∎

With finite domains, things are also very straightforward:

Lemma 19.4 (Cancellation laws)**.** *If R is a ring without zero divisors*[10] *then*

$$\forall a \neq 0, \forall b, c, \quad ab = ac \implies b = c \quad \text{and} \quad ba = ca \implies b = c$$

Proof. $ab = ac \implies a(b - c) = 0 \implies a = 0$ or $b - c = 0$. Since $a \neq 0$ we conclude that $b = c$. ∎

Theorem 19.5. *Every finite integral domain is a field.*

Proof. Suppose that R is a finite integral domain and let $a \in R$ be *non-zero.* Consider the function $f : R \to R$ defined by

$$f(x) = ax$$

By the cancellation laws,

$$f(x) = f(y) \implies ax = ay \implies x = y$$

whence f is injective. Since R is finite, it follows that f is *bijective.* But then $\exists b \in R$ such that $f(b) = 1$. Otherwise said, $ab = 1$ and so a is a unit. Since all non-zero elements are units, we have a field. ∎

Note where we needed the finiteness of R in order to drive the proof. The obvious counter-example of $R = \mathbb{Z}$ shows that an infinite integral domain need not be a field. Indeed, in such a case, the function $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto ax$ is injective, but is only *surjective* when $a = \pm 1$ is a unit.

Corollary 19.6. *$\mathbb{Z}_n$ is an integral domain if and only if n is prime. Indeed $a \in \mathbb{Z}_n$ is a zero-divisor if and only if* $\gcd(a, n) \neq 1$.

Factorizing polynomials

One of the upshots of this discussion is that one can factorize polynomials normally, even when working in $\mathbb{Z}_n$, but *only* if n is prime! We shall return to a formal discussion of polynomial rings later. For now, consider an example where $F = \mathbb{Z}_7$.

Given $3x^3 - 3x^2 + x - 1 = 0 \in \mathbb{Z}_7$, we start by trying solutions. Quickly we see that $x = 1$ works. Factorizing by $x - 1$ we obtain

$$3x^3 - 3x^2 + x - 1 = (x - 1)(3x^2 + 1)$$

[10] R need not be an integral domain, it could be non-commutative and might have no unity.

Keeping going: $x = 3$ solves $3x^2 + 1 = 0$, whence

$$3x^3 - 3x^2 + x - 1 = (x-1)(x-3)(3x+9) = 3(x-1)(x-3)(x+3)$$

We've obtained a complete factorization. Even though we found this by guessing solutions, the fact thar $\mathbb{Z}_7$ is an integral domain means that the only solutions arise from one of these factors being zero: the solutions are precisely $x = 1, 3, 4 \in \mathbb{Z}_7$.

Of course, we could simply have tried every element of $\mathbb{Z}_7$, so the method isn't very efficient when the ring is small.

What about solving equations in $\mathbb{Z}_n$ when n is composite? If $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$ is the unique prime decomposition, then

$$f(x) \equiv 0 \mod n \iff \forall i,\ f(x) \equiv 0 \mod p_i^{\mu_i} \implies \forall i,\ f(x) \equiv 0 \mod p_i$$

We can therefore start by breaking things up into individual primes. For example, to solve

$$x^3 + x^2 - 2 = 0 \in \mathbb{Z}_{18}$$

we first solve in $\mathbb{Z}_2$ and $\mathbb{Z}_3$. Thus

$$x^3 + x^2 = x^2(x+1) = 0 \implies x = 0, 1 \in \mathbb{Z}_2$$

and

$$x^3 + x^2 - 2 = (x-1)(x^2 + 2x + 2) = 0 \implies x = 1 \in \mathbb{Z}_3$$

Now extend to $\mathbb{Z}_9$: by the previous calculation we try $x = 1, 4$ and 7, of which only $x = 1$ works. It follows that $x = 0, 1 \in \mathbb{Z}_2$ and $x = 1 \in \mathbb{Z}_9$. Together these yield the solutions $x = 1, 10 \in \mathbb{Z}_{18}$.

Characteristics

Definition 19.7. Let R be a ring. Its *characteristic* $\mathrm{char}(R)$ is the smallest positive integer n such that

$$\forall a \in R,\ n \cdot a = \underbrace{a + \cdots + a}_{n \text{ times}} = 0$$

If no such n exists, we say the ring has characteristic zero.

Examples

1. It should be clear that $\mathrm{char}(\mathbb{Z}_n) = n$. Certainly

   $$\forall a,\ n \cdot a = na = 0 \in \mathbb{Z}_n$$

   Moreover, n is the least such number, since $k \cdot 1 = 0 \iff n \mid k$.

2. In the infinite rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ we have $k \cdot 1 = k$ which is never zero, whence these rings have characteristic zero.

The focus on what happens to 1 really is the whole story (at least in rings with unity!).

Theorem 19.8. *Suppose that R is a ring with unity. If $n \in \mathbb{N}$ is the least number such that $n \cdot 1 = 0$, then n is the characteristic of R. Otherwise said,* $\text{char}(R)$ *is the order of the cyclic subgroup $\langle 1 \rangle \leq (R, +)$ generated by 1.*

Proof. Observe that

$$n \cdot a = a + \cdots + a = a(1 + \cdots + 1) = a(n \cdot 1)$$

Thus $n \cdot 1 = 0 \iff n \cdot a = 0$ for all $a \in R$. ∎

Further Examples of Characteristics

1. The characteristic of $\mathbb{Z}_{15} \times \mathbb{Z}_{20}$ is the order of $(1, 1)$: this is $\text{lcm}(15, 20) = 60$.
2. If R is a commutative ring with characteristic 3, then
$$(a + b)^3 = a^3 + 3 \cdot a^2 b + 3 \cdot ab^2 + b^3 = a^3 + b^3$$
3. Let R be a ring and $M(R)$ be the set of 3×3 matrices with entries in R and whose first column is zero. This is a non-unital ring, even if R has a unity. Its characteristic is the same as that of R.

20 Fermat's and Euler's Theorems

Recall Theorem 18.7: If R is a ring with unity, then the set of units in R forms a *group under multiplication.* Applying this to $\mathbb{Z}_n$ recovers a famous discussion.

Definition 20.1. Let $\varphi(n) = |\mathbb{Z}_n^\times|$ denote the order of the group of units in $\mathbb{Z}_n$. The function $\varphi : \mathbb{N} \to \mathbb{N}$ is caller *Euler's totient function*.

Theorem 20.2 (Euler's Theorem). *If $a \in \mathbb{Z}_n^\times$ is a unit, then $a^{\varphi(n)} \equiv 1 \mod n$.*

Proof. By Lagrange's Theorem, the order k of an element a divides the order of the group $\varphi(n)$. Thus $k = \frac{\varphi(n)}{d}$ for some d. But then

$$a^{\varphi(n)} \equiv \left(a^k\right)^d \equiv 1^d \equiv 1 \mod n$$

∎

This result is known as *Fermat's Little Theorem* if n is prime (then $\mathbb{Z}_p^\times$ has order $\varphi(p) = p - 1$). The theorems of Fermat and Euler, and the function φ, have many applications, particularly in Number Theory. Here are a few highlights.

Theorem 20.3 (Computing φ).

1. *If p is prime, then $\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$.*
2. *Euler's function is* multiplicative*: that is,*
$$\gcd(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

3. *For any positive integer $n \geq 2$,*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Sketch Proof. 1. An element of $\mathbb{Z}_{p^k}$ is relatively prime to p^k if and only if it is *not* divisible by p. The remainders divisible by p all have the form

$$sp \quad \text{where} \quad s \in \{0, 1, 2, \ldots, p^{k-1} - 1\}$$

In particular, there are p^{k-1} remainders divisible by p, and so $\varphi(p^k) = p^k - p^{k-1}$ remainders which are not.

2. Take a course in number theory if you want to see a full argument for this! Here is an easy special case. Suppose $p \neq q$ are distinct primes. If $x \in \mathbb{Z}_{pq}$ is non-zero, then $\gcd(x, pq) = 1, p$ or q. It should be clear that

$$\begin{aligned} &\gcd(x, pq) = p \iff x = sp \quad \text{where} \quad s \in \{1, 2, \ldots, q-1\} \quad \text{and,} \\ &\gcd(x, pq) = q \iff x = tq \quad \text{where} \quad t \in \{1, 2, \ldots, p-1\} \end{aligned}$$

and that there is no overlap between these lists. Since $0 \in \mathbb{Z}_{pq}$ is not a unit, it follows that the number of non-units in $\mathbb{Z}_{pq}$ is

$$\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$$

3. This follows immediately from 1 and 2: given the unique prime factorization

$$n = p_1^{\mu_1} \cdots p_k^{\mu_k} \implies \varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\mu_i}) = \prod_{i=1}^{k} p_i^{\mu_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

■

Example: computing large powers To compute $197^{2018} \in \mathbb{Z}_{200}$, note first that $\varphi(200) = 200 \cdot \frac{1}{2} \cdot \frac{4}{5} = 80$ and that $\gcd(197, 200) = 1$, so that 197 is a unit. But then Euler's Theorem tells us that

$$197^{2018} = 197^{80 \cdot 25 + 18} = (197^{80})^{25} \cdot 197^{18} = 3^{18}$$

A little computation shows that $3^3 = 27,\ 3^6 = 129,\ 3^{12} = 41,\ 3^{18} = 89$ whence $197^{2018} = 89 \in \mathbb{Z}_{200}$.

Example: solving congruences To solve a congruence such as $x^7 \equiv 5 \mod 33$ we could laboriously check for *every* value of $x \in \mathbb{Z}_{33}$. Instead, suppose a solution x exists and let $d = \gcd(x, 33)$. Then $d \mid x^7$, and so $d \mid 5$. But this means that d is a common divisor of 5 and 33: d must be 1! It follows that any possible solution is a *unit.*
To apply Euler's Theorem requires a little trick: we want to raise both sides of the original equation to a power u such that $7u \equiv 1 \mod \varphi(33)$. That is,

$$7u \equiv 1 \mod 20 \implies 21u \equiv 3 \mod 20 \implies u \equiv 3 \mod 20$$

Now apply Euler's Theorem:

$$x^7 \equiv 5 \implies x^{21} \equiv 5^3 \implies x \equiv 5^3 \equiv 25 \cdot 5 \equiv -8 \cdot 5 \equiv 26 \mod 33$$

The structure of the group of units: non-examinable/open-book

The group of units in the ring $\mathbb{Z}_n$ is somewhat complicated: in general it can be quite difficult to identify the group structure. We do have the following result, which we state without proof.

Theorem 20.4. *$\mathbb{Z}_n^\times$ is cyclic if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime.*

Definition 20.5. If $\mathbb{Z}_n^\times$ is cyclic, any generator is termed a *primitive root* modulo n.

Corollary 20.6. *If g is a primitive root modulo n, then g^s is a primitive root if and only if $\gcd(\varphi(n), s) = 1$. In particular, there are $\varphi(\varphi(n))$ primitive roots.*

Proof. This is immediate from our knowledge of subgroups of cyclic groups. If g is a primitive root modulo n, then $\mathbb{Z}_n^\times = \langle g \rangle$. The cyclic subgroup $\langle g^s \rangle$ has order $\frac{\varphi(n)}{\gcd(\varphi(n),s)}$. ■

Examples

1. $n = 14$ has a primitive root, namely $g = 3$. We check

   $$\langle 3 \rangle = \{3, 9, 13, 11, 5, 1\} = \mathbb{Z}_{14}^\times$$

   There are $\varphi(\varphi(14)) = \varphi(6) = 2$ primitive roots, the other being 5. The group of units is isomorphic to $\mathbb{Z}_6$.

2. $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ is not cyclic. Since every element is its own inverse, we conclude that $\mathbb{Z}_8^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the Klein 4-group.

Finally, recall Corollary 18.10, if $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ is a ring isomorphism and so units correspond. Moreover $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a unit if and only if $x \in \mathbb{Z}_m^\times$ and $y \in \mathbb{Z}_n^\times$ (its inverse is $(x, y)^{-1} = (x^{-1}, y^{-1})$). We can easily generalize:

Corollary 20.7. *If $n = p_1^{\mu_1} \times \cdots \times p_k^{\mu_k}$ is the unique prime factorization of n, then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\mu_1}} \times \cdots \times \mathbb{Z}_{p_k^{\mu_k}}$$

is a ring isomorphism and

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{\mu_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{\mu_k}}^\times$$

is a group isomorphism.

Example $\mathbb{Z}_{65}^\times$ has order $\varphi(65) = 65 \cdot \frac{4}{5} \cdot \frac{12}{13} = 48$. By the Corollary,

$$\mathbb{Z}_{65}^\times = \mathbb{Z}_{5\cdot 13}^\times \cong \mathbb{Z}_5^\times \times \mathbb{Z}_{13}^\times \cong \mathbb{Z}_4 \times \mathbb{Z}_{12}$$

since both 5 and 13 are prime.

21 The Field of Quotients of an Integral Domain

A *field* is the closest one can get to having a set $(F, +, \cdot)$ which is an abelian group with respect to *two distinct distributing operations*: we always have to exclude at least 0 from the multiplicative group structure. Fields, and the ability to divide, are so useful that it is helpful to be able to embed any integral domain in a field. Essentially we wish to do the following:

> Given an integral domain D, find the *smallest field* F such that D is isomorphic to a subdomain of F.

Here is the approach whereby we construct $\mathbb{Q}$ from $\mathbb{Z}$. This is lengthy, but worth the read!

1. Define a relation $\sim$ on $S := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by

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

2. Prove that $\sim$ is an equivalence relation on S:

Reflexivity $\forall (a, b) \in S, ab = ba \implies (a, b) \sim (a, b)$.

Symmetry $\forall (a, b), (c, d) \in S$,

$$(a, b) \sim (c, d) \implies ad = bc \implies cb = da \implies (c, d) \sim (a, b)$$

Transitivity $\forall (a, b), (c, d), (e, f) \in S$,

$$\begin{aligned} (a, b) \sim (c, d) \text{ and } (c, d) \sim (e, f) &\implies ad = bc \text{ and } cf = de \\ &\implies adcf = bcde \implies cd(af - be) = 0 \\ &\implies c(af - be) \qquad\qquad (\text{since } d \in \mathbb{Z} \setminus \{0\}) \\ &\implies c = 0 \text{ or } af = be \\ &\implies c = 0 \text{ or } (a, b) \sim (e, f) \end{aligned}$$

However, if $c = 0$, then $a = 0 = e$ (since $d \neq 0$), in which case $af = be$ and we still have $(a, b) \sim (e, f)$.

3. Define $\mathbb{Q} = {}^{S}\!\big/_{\sim} = \{[(a, b)] : (a, b) \in S\}$ to be the set of equivalence classes of $\sim$ in S. We claim that $\mathbb{Q}$ inherits a field structure from $\mathbb{Z}$ in a natural way. Define operations $+$ and $\cdot$ on $\mathbb{Q}$ by

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)], \qquad [(a, b)] \cdot [(c, d)] := [(ac, bd)]$$

- These are well-defined operations: if $(a, b) \sim (p, q)$ and $(c, d) \sim (r, s)$, then $aq = bp$ and $cs = dr$. But then

$$[(p, q)] + [(r, s)] = [(ps + qr, qs)]$$

However,

$$\begin{aligned} &(ad + bc)qs - bd(ps + qr) = (aq - bp)ds + (cs - dr)bq = 0 \\ &\qquad \implies [(p, q)] + [(r, s)] = [(a, b)] + [(c, d)] \end{aligned}$$

Similarly,

$$acqs - bdpr = aqcs - aqcs = 0 \implies [(p, q)] \cdot [(r, s)] = [(a, b)] \cdot [(c, d)]$$

It follows that $\mathbb{Q}$ is closed under both operations.

- The operations are associative. This is tedious: it suffices to observe that

$$[(a,b)] + [(c,d)] + [(e,f)] = [(adf + bcf + bde, bdf)] \quad \text{and,}$$
$$[(a,b)] \cdot [(c,d)] \cdot [(e,f)] = [(ace, bdf)]$$

  regardless of which operation one computes first.
- The operations are commutative: this is immediate by inspection.
- Both operations have identities:

$$0_{\mathbb{Q}} = [(0,1)], \qquad 1_{\mathbb{Q}} = [(1,1)]$$

- Both operations have inverses:

$$-[(a,b)] = [(-a,b)], \qquad [(c,d)]^{-1} = [(d,c)] \qquad \text{(provided } [(c,d)] \neq 0_{\mathbb{Q}}\text{)}$$

- The distributive laws hold: for instance,

$$\begin{aligned}\big([(a,b)] + [(c,d)]\big) \cdot [(e,f)] &= [(ad+bc, bd)] \cdot [(e,f)] \\ &= [(ade + bce, bdf)] = [(adef + bcef, bdf^2)] \\ &= [(ae, bf)] + [(ce, df)] \\ &= [(a,b) \cdot [(e,f)] + [(c,d)] \cdot [(e,f)]\end{aligned}$$

  The other is similar.

The upshot is that we've *defined a field* $(\mathbb{Q}, +, \cdot)$. Of course it is customary to write $\frac{a}{b} = [(a,b)]$ so that the addition and multiplication operations become the familiar expressions

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

but we keep the old notation just a while longer...

4. Observe that the subring $\widehat{\mathbb{Z}} := \{[(a,1)] : a \in \mathbb{Z}\}$ is isomorphic to $\mathbb{Z}$. For this, define the function

$$\mu : \mathbb{Z} \to \widehat{\mathbb{Z}} : a \mapsto [(a,1)]$$

and check that μ is an isomorphism of rings.

Bijectivity μ is certainly surjective by definition. Moreover,

$$\mu(a) = \mu(b) \implies (a,1) \sim (b,1) \implies a \cdot 1 = 1 \cdot b \implies a = b$$

whence μ is injective.

Homomorphism It is easy to check that

$$\mu(a+b) = [(a+b,1)] = [(a,1)] + [(b,1)] = \mu(a) + \mu(b)$$
$$\mu(ab) = [(ab,1)] = [(a,1)] \cdot [(b,1)] = \mu(a) \cdot \mu(b)$$

The result is that we've *defined* a field $\mathbb{Q}$ containing an isomorphic copy of the integral domain $\mathbb{Z}$.

Generalizing So far, so exciting: we've laboriously defined and checked the consistency of an object $\mathbb{Q}$ with which we've been working for years. The next observation is crucial: check *every* step of the argument:

To construct $\mathbb{Q}$, all we required was that $\mathbb{Z}$ be an *integral domain*!

The lack of zero-divisors is required to prove the transitivity of $\sim$ while the fact that $\mathbb{Z}$ is a commutative ring is needed repeatedly.[11] The upshot is that we can repeat the construction for *any integral domain.*

Definition 21.1. Let D be an integral domain. Define the equivalence relation $\sim$ on $S = D \times (D \setminus \{0\})$ by

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

The *field of quotients* $\mathrm{Frac}(D)$ of D is the field $S/\sim$ with operations

$$[(a,b)] + [(c,d)] := [(ad+bc, bd)], \qquad [(a,b)] \cdot [(c,d)] := [(ac, bd)]$$

The notation is unwieldy, but before we can make everything simpler we need to prove perform one piece of housekeeping.

Theorem 21.2.

1. *Everything in the definition is as claimed: $\sim$ is an equivalence relation, the operations are well-defined and $\mathrm{Frac}(D)$ really is a field.*
2. *The subring*

   $$R = \{[(a,1)] : a \in D\}$$

   is ring-isomorphic to D.
3. *If L is any field containing D as a subring, then there exists a function $\psi : \mathrm{Frac}(D) \to L$ such that*
   - *(a) ψ is an isomorphism of $\mathrm{Frac}(D)$ onto a subfield of L,*
   - *(b) $\forall a \in D$, $\psi([(a,1)]) = a$.*

Remarks and Notation

- We've proved parts 1 and 2 in the above discussion: simply replace $\mathbb{Z}$ with D, $\mathbb{Q}$ with $\mathrm{Frac}(D)$ and $\widehat{\mathbb{Z}}$ with R.
- Atfer completing the proof, we will typically write ab^{-1} for the element $[(a,b)] \in \mathrm{Frac}(D)$. Under this identification, we see that $a = [(a,1)]$ for every $a \in D$, whence parts 2. and 3. become $R = D$ and $\psi(a) = a$.

[11] It might appear that the existence of the unity $1 \in \mathbb{Z}$ is required to define $0_{\mathbb{Q}}$, $1_{\mathbb{Q}}$ and to identify $\widehat{\mathbb{Z}} \leq \mathbb{Q}$, but these can be done via

$$0_{\mathbb{Q}} := [(0,b)], \qquad 1_{\mathbb{Q}} := [(b,b)], \qquad \widehat{\mathbb{Z}} = \{[(ab,b) : a \in \mathbb{Z}\}$$

where b is *any* non-zero integer. The construction is therefore valid in any commutative ring with no zero-divisors.

Proof of 3. Wtart by defining ψ. Since $D \leq L$, we see that *every non-zero element of D is invertible in the field L*. It follows that we can define

$$\psi([(a,b)]) = ab^{-1}$$

where ab^{-1} is computed in L. Now observe that

$$\begin{aligned}[(a,b)] = [(c,d)] &\iff (a,b) \sim (c,d) \iff ad = bc \\ &\iff ab^{-1} = b^{-1}a = cd^{-1} \\ &\iff \psi([(a,b)]) = \psi([(c,d)])\end{aligned}$$

whence ψ is well-defined and injective. We also clearly have $\psi([(a,1)]) = a \in L$. Moreover,

$$\psi([(a,b)] + \psi([(c,d)]) = ab^{-1} + cd^{-1} = (ad+bc)(bd)^{-1} = \psi([(a,b)] + [(c,d)])$$

and

$$\psi([(a,b)] \cdot \psi([(c,d)]) = ab^{-1}cd^{-1} = (ac)(bd)^{-1} = \psi([(a,b)] \cdot [(c,d)])$$

whence ψ is an isomorphism onto its image. ∎

The third part of the theorem is hugely important: it says that $\text{Frac}(D)$ is the *smallest field* containing D in the sense that every field containing D must contain an isomorphic copy of $\text{Frac}(D)$.

Examples

1. Suppose that D is already a field (this is automatic if D is a *finite* integral domain). Revisit the construction:

   $$(a,b) \sim (c,d) \iff ad = bc \iff ab^{-1} = cd^{-1} \text{ in } D!$$

   It follows that *the field of quotients is (isomorphic to) D itself.*

2. Consider the integral domain $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Its field of quotients consists of all elements

   $$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}$$

   so that we obtain the field[12]

   $$\mathbb{Q}(\sqrt{2}) := \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$$

[12]One can easily obtain any element of $\mathbb{Q}(\sqrt{2})$ by setting $d = 0$ and taking c to be the least common multiple of the denominators of p, q.