Summary of results:
Commutative rings

Alan Haynes, haynes@math.uh.edu
Last update: January 26, 2022

1. Rings, ideals, fields

A **ring** is a set R together with binary operations $+$ and $\cdot$ satisfying the following properties:

(i) $(R, +)$ is an Abelian group. The identity element of this group is called the additive identity and is denoted by 0.

(ii) For any $a, b, c \in R$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, and

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$, and

(iv) $(a + b) \cdot c = a \cdot c + b \cdot c$.

If multiplication commutes, i.e. for every $a, b \in R$ we have $a \cdot b = b \cdot a$, then R is a **commutative ring**. If there is an element $1 \in R$ with the property that, for any $a \in R$, we have $1 \cdot a = a \cdot 1 = a$, then 1 is called the multiplicative identity of R (if it exists, it must be unique) and R is a **ring with identity**. *In all of what follows, we will assume that R is a commutative ring with identity.*

From now on we will write $a \cdot b$ as ab. We say that an element $a \in R$ has a multiplicative inverse if there exists a $b \in R$ for which $ab = 1$. The set of elements of a ring R which have multiplicative inverses are called the **units** of R, denoted by $R^\times$. The set $R^\times$ forms a group under multiplication. For any two elements $a, b \in R$, if there is a unit $u \in R^\times$ for which $a = ub$, then we say that a and b are **associate** in R.

A non-zero element $a \in R$ is called a **zero-divisor** if there is another nonzero element $b \in R$ such that $ab = 0$. A non-zero commutative ring (i.e. $R \neq \{0\}$) with no zero-divisors is called an **integral domain**, which we will abbreviate as ID. Examples of ID's are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$ (where p is a prime number), and $\mathbb{Z}[x]$. Furthermore, if R is an ID then so is $R[x]$ (and the implication trivially goes the other direction as well). Examples of commutative rings which are not ID's are $\mathbb{Z}/n\mathbb{Z}$, when n is a composite number.

Suppose that $a, b \in R$. We say that a is a **multiple** of b, and that b **divides** a, if there exists $c \in R$ for which $a = bc$. One notation for this is to write $b \mid a$. An element $d \in R$ is called a **common divisor** of a and b if $d \mid a$ and $d \mid b$. A common divisor d is called a **greatest common divisor (gcd)** if for every other common divisor

d' of a and b, we have that $d' \mid d$. In general, two elements a and b in a commutative ring R may have several gcd's, or they may have none.

An **ideal** in R is a set $I \subseteq R$ which satisfies the following properties:

(i) $(I, +)$ is a group, and

(ii) for every $r \in R$ and $x \in I$, we have $rx \in I$.

Examples of ideals are the sets

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} \subseteq \mathbb{Z},$$

where n is an integer,

$$f(x)R[x] = \{f(x)g(x) : g(x) \in R[x]\} \subseteq R[x],$$

where $f(x) \in R[x]$, and

$$\{f(x) \in \mathbb{Z}[x] : 2|f(0)\} \subseteq \mathbb{Z}[x].$$

In any ring R the sets $\{0\}$ and R are always ideals. An example of a set which is not an ideal is the subset $\mathbb{Z}$ of the ring $\mathbb{Q}$. Note that $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and it is true that for every $r \in \mathbb{Z}$ and $x \in \mathbb{Z}$, we have $rx \in \mathbb{Z}$. However, property (ii) in the definition of 'ideal' is required to hold *for all* $r \in R$, not just for $r \in I$. In other words, an ideal has to 'absorb multiplication' from all elements of R (which doesn't happen in the example just given). This is important for making sure that the quotient ring, which we will come to next, is well defined.

Suppose that I is an ideal in R. Then $(I, +)$ is a subgroup of the group $(R, +)$, so the collection of all cosets $x + I$, with $x \in R$, forms a group under addition (note that $(R, +)$ is an Abelian group, so every subgroup is automatically normal). For each $x, y \in R$ we *define* the product of the cosets $x + I$ and $y + I$ by

$$(x + I) \cdot (y + I) = xy + I.$$

As a technical point, we emphasize that this is the definition of a binary operation on the collection of cosets, and it does not in general indicate an equality between two sets of objects. To see why it is well defined, notice that if $x' \in x + I$ and $y' \in y + I$ then $x' = x + a$ and $y' = y + b$ for some $a, b \in I$, and

$$x'y' + I = xy + ay + bx + ab + I = xy + I,$$

since, using the properties in the definition of ideal, ay, bx, and ab are all elements of the additive group I. Now it is not difficult to check that the collection of all cosets of I in R, together with the operations of coset addition and multiplication, forms a commutative ring with identity, called the **quotient ring** of R by the ideal I, and denoted

by R/I. The additive identity in R/I is $0+I$, and the multiplicative identity is $1+I$.

A **ring homomorphism** from a ring R to a ring S is a function $\varphi : R \to S$ with the properties that, for all $a, b \in R$,

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{and} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

The **kernel** of φ, denoted $\ker(\varphi)$, is defined by

$$\ker(\varphi) = \{a \in R : \varphi(a) = 0\}.$$

If φ is a bijective homomorphism then it is called an **isomorphism**, and R and S are said to be ring **isomorphic**, denoted $R \cong S$. One key fact about ring homomorphisms is the First Isomorphism Theorem for Rings, which says that, if $\varphi : R \to S$ is a ring homomorphism then:

(i) $\varphi(R)$ is a subring of S,

(ii) $\ker(\varphi)$ is an ideal in R, and

(iii) We have that

$$R/\ker(\varphi) \cong \varphi(R),$$

and the map $\tau : R/\ker(\varphi) \to \varphi(R)$ defined by

$$\tau(x + \ker(\varphi)) = \varphi(x)$$

is an isomorphism.

Next, a **field** is an integral domain in which every non-zero element has a multiplicative inverse. Familiar examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ when p is a prime. Examples of ID's which are not fields are $\mathbb{Z}$ and $\mathbb{Q}[x]$. Now, although an integral domain R can in general fail to be a field, an isomorphic copy of R will always be contained in a field called its **field of fractions**. The construction of the field of fractions of an integral domain R is exactly analogous to the way that we construct $\mathbb{Q}$ from $\mathbb{Z}$. Let $\mathcal{Q}$ be the subset of the Cartesian product $R \times R$ defined by

$$\mathcal{Q} = \{(a, b) : a, b \in R, b \neq 0\},$$

and define an equivalence relation $\sim$ on $\mathcal{Q}$ by setting

$$(a, b) \sim (a', b') \quad \text{if and only if} \quad a'b = ab'.$$

We leave it to the reader to check that this is an equivalence relation. Let $F = \mathcal{Q}/\sim$ be the collection of equivalence classes (which we will denote with square brackets as $[a, b]$) and define two binary operations, addition and multiplication, on F, by

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [a, b] \cdot [c, d] = [ac, bd].$$

It is easy to check that these definitions do not depend on the choice of representatives for the equivalence classes involved. Furthermore, the fact that R is an integral domain guarantees that bd is non-zero (since b and d are non-zero), so everything is well defined. The set F together with these two operations forms a commutative ring with identity. The additive inverse is $[0,1]$ and the multiplicative inverse is $[1,1]$. If

$$[a,b]\cdot[c,d]=[ac,bd]=[0,1]$$

then, using the definition of the equivalence relation, we must have that $ac=0$, so $a=0$ or $c=0$. It follows that $(a,b)\sim(0,1)$ or $(c,d)\sim(0,1)$, in other words $[a,b]=[0,1]$ or $[c,d]=[0,1]$. This argument shows that F is an integral domain. Actually, if $[a,b]$ is any element of F and $[a,b]\neq[0,1]$ then $a\neq 0$ and the element $[b,a]$ is a multiplicative inverse for $[a,b]$. In other words, F is a field. Finally, the map $\varphi: R\to F$ defined by $\varphi(a)=[a,1]$ is a ring homomorphism with kernel equal to $\{0\}$. This means that $\varphi(R)\cong R$, so F contains an isomorphic copy of R. The field F is what we call the field of fractions of R, and it is also the smallest field containing (an isomorphic copy of) R.

Suppose that F is a field and that $I\subseteq F$ is an ideal of F. If I contains a non-zero element a of F then (by property (ii) in the definition of ideal) the element $a^{-1}a=1$ must also lie in I. But if 1 is in I then (again by property (ii)) we must have that $I=F$. This shows that the only ideals in F are $\{0\}$ and F. In fact it is not difficult to see that this property characterizes fields, in the sense that a commutative ring R with identity is a field if and only if the only ideals of R are $\{0\}$ and R.

A proper ideal $I\subseteq R$ (i.e. $I\neq R$) is called **maximal** if there are no other proper ideals J in R which contain I. It can be proven, using the conclusion of the previous paragraph, that a proper ideal I in a commutative ring R is maximal if and only if the quotient ring R/I is a field. We leave the proof as an exercise.

A proper ideal $I\subseteq R$ (i.e. $I\neq R$) is called **prime** if it has the property that, whenever $a,b\in R$ and $ab\in I$, then it follows that $a\in I$ or $b\in I$. It is not difficult to show that any maximal ideal is prime, but the converse is not true in general. It is also true that a proper ideal $I\subseteq R$ is prime if and only if the quotient ring R/I is an ID.

2. UFD's, PID's, and ED's

In this section we will assume, even if not explicitly stated, that the ring R is an integral domain.

We say that a non-zero, non-unit element $a \in R$ is **irreducible** if it cannot be written as the product of two non-units. Otherwise we say that a is **reducible**. As examples, the prime numbers are irreducible elements in the ring $\mathbb{Z}$, and the polynomial $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$ (but not in $\mathbb{C}[x]$). As another example, in a field there are no irreducible elements, since every non-zero element is a unit.

We say that an ID R is a **unique factorization domain**, abbreviated UFD, if every non-zero element $a \in R$ can be written in the form

$$a = up_1p_2 \cdots p_k,$$

where $u \in R^\times$, the elements $p_1, \ldots, p_k$ are irreducible, and where this representation is unique up to rearrangement of the terms and replacement of the factors by associates. An example which most people are familiar with is the fact that the ring $\mathbb{Z}$ is a UFD. This is the fundamental theorem of arithmetic. However, there are many interesting ID's which are not UFD's.

If $\mathcal{A} \subseteq R$ then the **ideal generated by** $\mathcal{A}$, denoted by $(\mathcal{A})$, is the smallest ideal of R which contains $\mathcal{A}$. Since R itself is an ideal of R containing $\mathcal{A}$, and since the intersection of an arbitrary number of ideals is itself an ideal (proof left to reader), the ideal generated by $\mathcal{A}$ always exists and is equal to the intersection of all ideals of R containing $\mathcal{A}$. It can also be written down conveniently as

$$(\mathcal{A}) = \{r_1a_1 + \cdots + r_na_n : n \in \mathbb{N}, r_1, \ldots r_n \in R, a_1, \ldots a_n \in \mathcal{A}\},$$

the collection of all finite linear combinations of elements of $\mathcal{A}$, with coefficients taken from R.

Suppose $I \subseteq R$ is an ideal. If there exists an $a \in R$ such that $I = (a)$ then I is called a **principal ideal**. In this case we have that

$$I = \{ra : r \in R\}.$$

An example of ideal which is not a principal ideal is the ideal in $\mathbb{Z}[x]$ generated by the set $\{2, x\}$ (this ideal is also one of the examples given after the definition of 'ideal' above). A commutative ring in which every ideal is principal is called a **principal ideal domain**, or PID for short.

Finally, an integral domain R is called a **Euclidean domain**, abbreviated ED, if there is a function $\phi : R \setminus \{0\} \to \mathbb{N}$ with the property that for any $a, b \in R$ with $b \neq 0$, there exist elements $q, r \in R$ with

$$a = qb + r \quad \text{and either} \quad r = 0 \quad \text{or} \quad \phi(r) < \phi(b).$$

Examples of Euclidean domains include the integers and polynomial rings $F[x]$, whenever F is a field. In the integers, ϕ can be taken to be the absolute value map, and then the requirement above is satisfied because of the division algorithm. In the polynomial rings $F[x]$ (with F a field) the function ϕ can be taken to be the degree map (this is justified by the division algorithm for polynomials with coefficients in a field).

One important result relating the above definitions is that we have the following heirarchy:

$$(\text{ED}) \Rightarrow (\text{PID}) \Rightarrow (\text{UFD}).$$

For example, it follows from this that if F is a field then (since $F[x]$ is an ED), $F[x]$ is a PID and a UFD. On the other hand, $\mathbb{Z}[x]$ is not a PID (as mentioned above), so it is not an ED. Note, however that $\mathbb{Z}[x]$ is a UFD. In fact it follows from Gauss's Lemma that $R[x]$ is a UFD whenever R is a UFD.