Chapter 1 : A primer on ideals

In these notes, we concentrate only on *commutative rings* often without specific mention.

1.1 Definition Let R be a ring (commutative). A subset $\mathfrak{a} \subseteq R$ is called an *ideal* of R if:

(i) $\mathfrak{a}$ is a subgroup of $(R, +)$, and
(ii) $\mathfrak{a}$ is closed under multiplication by elements of R, i.e., $ra \in \mathfrak{a}$ for all $r \in R$ and $a \in \mathfrak{a}$.

1.2 Example

(1) The set $\{0\}$ is the trivial subgroup of $(R, +)$. Moreover, $r \cdot 0 = 0$ for all $r \in R$. Thus the set $\{0\}$ is an ideal of R and is called the *zero ideal*, denoted by 0.

(2) On the other extreme, the entire set R is clearly an ideal of R and is called the *unit ideal* of R. The name is attributed to the following proposition.

1.3 Proposition Let $\mathfrak{a}$ be an ideal of R. Then $\mathfrak{a}$ is the unit ideal if and only if $\mathfrak{a}$ contains a unit of R.

Proof [Only if] If $\mathfrak{a} = R$, then $1 \in \mathfrak{a}$.

[If] Let $\mathfrak{a}$ contain a unit u. There exists $v \in R$ such that $uv = 1$. By the second property of ideals, we then have $1 \in \mathfrak{a}$. Moreover, for any $r \in R$ we have $r = r \cdot 1 \in \mathfrak{a}$ again by the second property of ideals. Therefore, $R \subseteq \mathfrak{a}$. ◄

1.4 Corollary The only ideals of a field F are the zero ideal and the unit ideal.

Proof Let $\mathfrak{a}$ be a non-zero ideal of F, i.e., let $\mathfrak{a}$ contain a non-zero element a. Since F is a field, a is a unit of F, i.e., $\mathfrak{a}$ is the unit ideal. ◄

(3) Take $R = \mathbb{Z}$ and $n \in \mathbb{Z}$. All integer multiples of n form an ideal of $\mathbb{Z}$ denoted by $n\mathbb{Z}$ or $\langle n \rangle$.

$$\langle n \rangle = n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}.$$

We call $\langle n \rangle$ the *principal ideal* generated by n. We will later see that every ideal of $\mathbb{Z}$ is a principal ideal.

(4) Let us generalize the concept of Part (3). Let R be any ring (of course, commutative) and $a \in R$. Then the ideal generated by a is defined as

$$Ra = \langle a \rangle = \{ra \mid r \in R\}.$$

More generally, let $a_1, a_2, \ldots, a_n \in R$. The set of all finite linear combinations of $a_1, a_2, \ldots, a_n$ is an ideal of R.

$$Ra_1 + Ra_2 + \cdots + Ra_n = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

The notation $\langle \cdots \rangle$ is ambiguous, since it does not mention the ring in which ideals are considered. We can use this notation in case the ring R is clear from the context.

For $R = \mathbb{Z}$ the ideal $\langle 4, 6\rangle = \{4a + 6b \mid a, b \in \mathbb{Z}\}$ is also equal to $\langle 2\rangle = \{2a \mid a \in \mathbb{Z}\}$. As mentioned earlier, every ideal of $\mathbb{Z}$ is a principal ideal. It can be proved that if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ are not all zero, then $\langle a_1, a_2, \ldots, a_n\rangle$ is the principal ideal generated by $\gcd(a_1, a_2, \ldots, a_n)$.

All ideals need not be principal. Consider $R = \mathbb{Z}[x]$ and $\mathfrak{a} = \langle x, 2\rangle$. Then $\mathfrak{a}$ consists of polynomials of the form $xf(x) + 2g(x)$ with $f(x), g(x) \in \mathbb{Z}[x]$. It is easy to see the $\mathfrak{a}$ consists precisely of those polynomials of $\mathbb{Z}[x]$ in which the constant term is even. This ideal is not principal. In order to prove this, let us assume otherwise, i.e., $\mathfrak{a} = \langle h(x)\rangle$ for some $h(x) \in \mathbb{Z}[x]$. Since x and 2 belong to $\mathfrak{a}$, $h(x)$ divides both x and 2 and so must be equal to ± 1. But then $h(x)$ is a unit and so we must have $\mathfrak{a} = \mathbb{Z}[x]$, a contradiction to the fact that $\mathfrak{a}$ does not contain polynomials with odd constant terms.

(5) Let $R = \mathbb{Z}_n$ and $a \in \mathbb{Z}_n$. The principal ideal $\langle a\rangle$ of $\mathbb{Z}_n$ is equal to $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$. As a specific example, take $n = 10$. If $a = 2$, then the distinct multiples of a are $\{0, 2, 4, 6, 8\}$. This is a proper ideal of $\mathbb{Z}_{10}$. On the other hand, for $a = 3$ we have $\langle 3\rangle = \{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\} = \mathbb{Z}_{10}$.

1.5 Definition Let R be a ring. A subset $S \subseteq R$ is called a *subring* of R is S is a ring under the binary operations of R.

1.6 Example

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\mathbb{Q}$ is a subring (also a *subfield*) of $\mathbb{R}$ and $\mathbb{C}$. Finally, $\mathbb{R}$ is a subfield of $\mathbb{C}$.

(2) Every ring R is canonically embedded in the polynomial ring $R[x]$ (consider the constant polynomials). Thus R is a subring of $R[x]$.

Ideals and subrings are different concepts. A subring, being a ring, must contain the multiplicative identity, whereas the only ideal containing the multiplicative identity is the unit ideal. On the other hand, it suffices for a subring to be closed under multiplication by elements of the subring, whereas an ideal must be closed under multiplication by elements of the entire ring. For example, $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$, since $2 \times \frac{1}{3} \notin \mathbb{Z}$.

1.7 Definition An integral domain in which all ideals are principal is called a *principal ideal domain* or a *PID* in short.

1.8 Proposition $\mathbb{Z}$ is a PID.

Proof Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}$. If $\mathfrak{a} = 0$, then it is the principal ideal generated by the element 0. So assume that $\mathfrak{a} \neq 0$, i.e., $\mathfrak{a}$ contains non-zero integers. Since $a \in \mathfrak{a}$ if and only if $-a \in \mathfrak{a}$ ($\mathfrak{a}$ is a group under addition), $\mathfrak{a}$ contains *positive* integers. Let a be the smallest positive integer contained in $\mathfrak{a}$. I will show that $\mathfrak{a} = \langle a\rangle$. Since $\mathfrak{a}$ is closed under multiplication by integers and since $a \in \mathfrak{a}$, it is evident that $\langle a\rangle \subseteq \mathfrak{a}$. For proving the converse inclusion, take $b \in \mathfrak{a}$. Since $a \neq 0$, we can apply the Euclidean division algorithm to obtain $b = qa + r$ with $q, r \in \mathbb{Z}$ and $0 \leqslant r < a$. Since $a \in \mathfrak{a}$, $qa \in \mathfrak{a}$ too (property (ii)). Moreover, since $\mathfrak{a}$ is an additive group and $b \in \mathfrak{a}$, $r = b - qa \in \mathfrak{a}$. Now a has been chosen to be the smallest positive integer contained in $\mathfrak{a}$. So r cannot be positive, i.e., $r = 0$. But then $b = qa \in \langle a\rangle$, i.e., $\mathfrak{a} \subseteq \langle a\rangle$. ◀

The crux of the above proof lies in our ability to apply Euclidean division in R. An analogous proof for any ring R in which Euclidean division holds lets us conclude the general result:

1.9 Proposition Any ED (Euclidean domain) is a PID. In particular, $\mathbb{Z}$ and $F[x]$ (F a field) are PIDs. ◀

$\mathbb{Z}[x]$ is not a PID, since $\langle x, 2\rangle$ is not principal. That is not unexpected; $\mathbb{Z}$ is not a field anyway.

Ideals are instrumental for the construction of quotient rings. In this sense ideals play the same role as do normal subgroups in connection with groups.

Let R be a ring and $\mathfrak{a}$ an ideal of R. Since $(R, +)$ is Abelian, $\mathfrak{a}$ is a normal subgroup of $(R, +)$. The set

$$R/\mathfrak{a} = \{r + \mathfrak{a} \mid r \in R\}$$

of cosets of R with respect to $\mathfrak{a}$ is, therefore, an Abelian group under addition defined as

$$(r + \mathfrak{a}) + (s + \mathfrak{a}) = (r + s) + \mathfrak{a}.$$

We plan to define a multiplication in $R/\mathfrak{a}$ in the following way:

$$(r + \mathfrak{a})(s + \mathfrak{a}) = (rs) + \mathfrak{a}.$$

It is an easy check that this multiplication is well-defined, i.e., independent of the choice of the representatives of the equivalence classes $r + \mathfrak{a}$ and $s + \mathfrak{a}$. Under these addition and multiplication of cosets, $R/\mathfrak{a}$ becomes a ring called the *quotient ring* of R with respect to $\mathfrak{a}$. The coset $1 + \mathfrak{a}$ acts as the multiplicative identity of $R/\mathfrak{a}$. Since R is commutative, $R/\mathfrak{a}$ is commutative too.

1.10 Example

(1) Let $\mathfrak{a} = 0$. Then each coset of R is a singleton. Thus the quotient ring $R/\mathfrak{a}$ is essentially the same as the ring R.

(2) Next consider the unit ideal $\mathfrak{a} = R$. Now there is only one coset, namely R itself, and so the quotient ring $R/\mathfrak{a}$ is the zero ring. This is expected, since the additive identity $0 + R$ is the same as the multiplicative identity $1 + R$.

(3) Take $R = \mathbb{Z}$ and $\mathfrak{a} = \langle n \rangle$ for some $n \in \mathbb{N}$. The quotient ring $\mathbb{Z}/\langle n \rangle$ is essentially the same as the ring $\mathbb{Z}_n$ under addition and multiplication modulo n.

(4) Let F be a field and take $R = F[x]$. Choose a non-constant polynomial $f(x) \in F[x]$ and consider the principal ideal $\mathfrak{a}$ of $F[x]$ generated by $f(x)$. The quotient ring $S = F[x]/\langle f(x) \rangle$ deserves specific mention in this regard. I claim that S can be represented as the set:

$$S = \{a(x) \in F[x] \mid \deg a(x) < \deg f(x)\}.$$

To see why, take any $g(x) \in F[x]$. Euclidean division of $g(x)$ by $f(x)$ yields $g(x) = q(x)f(x) + r(x)$ with $\deg r(x) < \deg f(x)$. Since $q(x)f(x) \in \mathfrak{a}$, it follows that $g(x) + \mathfrak{a} = r(x) + \mathfrak{a}$. Thus every coset of $F[x]$ has a representative of degree less than $\deg f(x)$.

Furthermore, different representatives of degrees less than $\deg f(x)$ belong to different cosets. Consider $a(x), b(x) \in S$ with $\deg a < \deg f$ and $\deg b < \deg f$. If $a(x) + \mathfrak{a} = b(x) + \mathfrak{a}$, we have $a(x) - b(x) \in \mathfrak{a}$, i.e., $a(x) - b(x)$ is a multiple of $f(x)$. But $a(x) - b(x)$ is of degree strictly less than $\deg f$, and F is a field. Thus we must have $a(x) = b(x)$.

It is easy to check that the arithmetic of the quotient ring S is the arithmetic of $F[x]$ modulo the polynomial $f(x)$. The passage from $F[x]$ to $F[x]/\langle f(x) \rangle$ is perfectly analogous to the passage from $\mathbb{Z}$ to $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$.

1.11 Proposition Let F be a field and $f(x)$ a non-constant polynomial in $F[x]$. The quotient ring $S = F[x]/\langle f(x) \rangle$ is a field if and only if $f(x)$ is irreducible in $F[x]$.

Proof [If] Since F is commutative, S is also commutative. It suffices only to show that every non-zero element $a(x)+\mathfrak{a} \in S$ has an inverse in S. We can choose the representative $a(x)$ to be a non-zero polynomial

of degree less than $\deg f$. Since f is irreducible, $\gcd(a(x), f(x)) = 1$, and so by the extended gcd theorem there exist polynomials $u(x), v(x) \in F[x]$ such that $u(x)a(x) + v(x)f(x) = 1$. Since $v(x)f(x) \in \langle f(x)\rangle$, we have $(u(x) + \langle f(x)\rangle)(a(x) + \langle f(x)\rangle) = 1 + \langle f(x)\rangle$, i.e., $u(x) + \langle f(x)\rangle$ is the inverse of $a(x) + \langle f(x)\rangle$.

[Only if] Let $f(x)$ be reducible, i.e., $f(x) = g(x)h(x)$ for some non-constant polynomials $g(x), h(x) \in F[x]$. The degrees of g and h are less than $\deg f$, and so $g(x) + \langle f(x)\rangle$ and $h(x) + \langle f(x)\rangle$ are nonzero elements of S. Moreover, $(g(x) + \langle f(x)\rangle)(h(x) + \langle f(x)\rangle) = f(x) + \langle f(x)\rangle = 0 + \langle f(x)\rangle$, i.e., S is not even an integral domain, let alone a field. ◀

Irreducible polynomials play the same role for the ring $F[x]$ as prime numbers do in connection with the ring $\mathbb{Z}$.

1.12 Example

Take $F = \mathbb{R}$ and the irreducible polynomial $f(x) = x^2 + 1$. Look at the field $S = \mathbb{R}[x]/\langle x^2 + 1\rangle$. The elements of S can be represented by polynomials with real coefficients and of degrees < 2, i.e., as $a+bx$ for $a, b \in \mathbb{R}$. Addition of two such polynomials is simple: $(a+bx)+(c+dx) = (a+c)+(b+d)x$. Multiplication in S can be carried out as: $(a+bx)(c+dx) = ac+(ad+bc)x+bdx^2 = ac+(ad+bc)x-bd+bd(x^2+1) = (ac - bd) + (ad + bc)x$ (modulo $x^2 + 1$). That's quite familiar, eh? Multiplication of complex numbers! You are used to write i instead of x. In fact, since $x^2 + 1 = 0$ in S, x is indeed a square root of -1. To sum up, the field S is the algebraic description of the field $\mathbb{C}$ of complex numbers.

Irreducible polynomials thus have the capability of defining new fields from existing ones. A special class of fields finds immense applications in several engineering disciplines including error correcting coding and cryptography.

1.13 Definition A field F for which the size $|F|$ of the set F is finite is called a *finite field* or a *Galois field*.

We have seen $\mathbb{Z}_n$ is a field if and only if n is a prime. These are our first and easiest examples of finite fields. The technique of forming quotients of polynomial rings leads us to the algebraic description of other finite fields.

Start with the polynomial ring $F[x] = \mathbb{Z}_p[x]$, p a prime, and take $n \in \mathbb{N}$, $n \geqslant 2$. It is a deep result that for every prime p and every $n \in \mathbb{N}$, there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree n. Let $f(x)$ be such a polynomial. We have the quotient ring

$$K = \mathbb{Z}_p[x]/\langle f(x)\rangle = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_p\}$$

which is a field, since $f(x)$ is irreducible. We can choose each coefficient a_i in p different ways. Also for different choices of $a_0, a_1, \ldots, a_{n-1}$, we get different elements of K. To sum up, K is a field of size p^n, i.e., K is again a finite field. The arithmetic of K is the arithmetic of the polynomial ring $\mathbb{Z}_p[x]$ modulo the irreducible polynomial $f(x)$.

1.14 Example

(1) Take $p = 5$ and $n = 2$. Since $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ and $4^2 = 1$ in $\mathbb{Z}_5$, the polynomial $f(x) = x^2 + 2$ is irreducible in $\mathbb{Z}_5[x]$. Thus the quotient ring

$$K = \mathbb{Z}_5[x]/\langle x^2 + 2\rangle = \{a + bx \mid a, b \in \mathbb{Z}_5\}$$

is a field with $5^2 = 25$ elements. Addition in K is simple: $(2+3x)+(4+x) = (2+4)+(3+1)x = 1+4x$. For multiplication, we first multiply the operands as polynomials in $\mathbb{Z}_5[x]$. Then we reduce the product modulo

x^2+2. For instance, $(2+3x)(4+x) = 3+2x+2x+3x^2 = 3+4x+3x^2 = 3+4x+3(x^2+2)-3\times 2 = 3+4x-1 = 2+4x$.

(2) The polynomial x^3+x+1 is irreducible in $\mathbb{Z}_2[x]$ and so

$$K = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$$

is a finite field of size $2^3 = 8$. Its elements are $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$. The addition and multiplication tables for K are given below.

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Addition table

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Multiplication table

(3) The cryptographic algorithm AES (Advanced Encryption Standard) uses the finite field of $2^8 = 256$ elements defined as $\mathbb{Z}_2[x]/\langle x^8+x^4+x^3+x+1\rangle$.

Finite fields possess many interesting algebraic properties. A detailed discussion of these properties is well beyond the scope of this introductory course. Let me mention some salient points without proof.

For every prime p and every $n \in \mathbb{N}$ there exist finite fields of size p^n. Conversely, every finite field must be of size p^n for some prime p and some $n \in \mathbb{N}$. Moreover, any two finite fields of the same size are essentially the same (isomorphic). This enables us to talk about *the* (instead of *a*) finite field of size p^n and denote this field by the special symbols $\mathbb{F}_{p^n}$ and $\mathrm{GF}(p^n)$.

The multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ of every finite field $\mathbb{F}_q$ is cyclic. A generator of $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

1.15 Example

(1) First consider the prime field $\mathbb{F}_{17} = \mathbb{Z}_{17}$. The size of $\mathbb{F}_{17}^*$ is 16. So every element of $\mathbb{F}_{17}^*$ is of order 2^i for some $i \in \{0,1,2,3,4\}$. First consider the element 2. We have $2^1 = 2$, $2^2 = 4$, $2^4 = 16$ and $2^8 = 1$ in $\mathbb{F}_{17}$, i.e., 2 is not a primitive element of $\mathbb{F}_{17}$. On the other hand, $3^1 = 3$, $3^2 = 9$, $3^4 = 13$, $3^8 = 16$, $3^{16} = 1$ modulo 17, i.e., 3 is a primitive element of $\mathbb{F}_{17}$.

(2) The size of $\mathbb{F}_8^*$ is 7 (a prime), and so every element of $\mathbb{F}_8^*$ (other than 1) is a primitive element of $\mathbb{F}_8$. For example, the powers of x under the above representation of $\mathbb{F}_8$ are:

i	0	1	2	3	4	5	6	7
x^i	1	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

(3) The order of $\mathbb{F}_{25}^*$ is 24. So $\mathbb{F}_{25}^*$ consists of elements of orders $1, 2, 3, 4, 6, 8, 12, 24$. Consider the representation $\mathbb{F}_{25} = \mathbb{Z}_5[x]/\langle x^2+2\rangle$. The element x in this representation satisfies $x^1 = x$, $x^2 = 3$, $x^4 = 4$ and $x^8 = 1$, i.e., $\operatorname{ord} x = 8$, i.e., x is not a primitive element of $\mathbb{F}_{25}$. Now consider the element $x+1$. We have $(x+1)^1 = x+1$, $(x+1)^2 = 2x+4$, $(x+1)^3 = x$, $(x+1)^4 = x+3$, $(x+1)^6 = x^2+2$, $(x+1)^8 = x+2$, $(x+1)^{12} = 4$ and $(x+1)^{24} = 1$. That is, $x+1$ is a primitive element of $\mathbb{F}_{25}$.