CHAPTER 14

Ideals and Factor Rings

Ideals

DEFINITION (Ideal). A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$, $ra \in A$ and $ar \in A$.

NOTE.

(1) A "absorbs" elements of R by multiplication.

(2) Ideals are to rings as normal subgroups are to groups.

DEFINITION. An ideal A of R is a proper ideal if A is a proper subset of R.

THEOREM (Ideal Test). *A nonempty subset A of a ring R is an ideal of R if*

(1) $a, b \in A \Longrightarrow a - b \in A$.

(2) $a \in A$ *and* $r \in R \Longrightarrow ar \in A$ *and* $ra \in A$.

PROOF.

Follows directly from the definition of ideal and Theorem 12.3 (Subring Test). □

EXAMPLE.

(1) $\{0\}$ (the trivial ideal) and R itself are ideals of R.

(2) For any positive integer n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is an ideal of $\mathbb{Z}$.

(3) Let R be a commutative ring with identity and let $a \in R$. The set

$$\langle a \rangle = \{ra | r \in R\}$$

is an ideal of R called the <u>principal ideal generated by a</u>.

Note that the commutative assumption is necessary here. Also, context will distinguish between this use of $\langle a \rangle$ and its use in cyclic groups.

(4) Let $\mathbb{R}[x]$ denote the set of all poynomials with real coefficients and let A be the subset of all polynomials with constant term 0. Then A is an ideal of $\mathbb{R}[x]$ and $A = \langle x \rangle$.

(5) Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n \in R$. Then

$$I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n | r_i \in R\}$$

is an ideal of R called the <u>ideal generated by $a_1, a_2, \ldots, a_n$</u>.

PROOF.

If $r_1a_1 + r_2a_2 + \cdots + r_na_n,\ r'_1a_1 + r'_2a_2 + \cdots + r'_na_n \in I$,

$$\begin{aligned}(r_1a_1 + r_2a_2 + \cdots + r_na_n) - (r'_1a_1 + r'_2a_2 + \cdots + r'_na_n) = \\ (r_1a_1 - r'_1a_1) + (r_2a_2 - r'_2a_2) + \cdots + (r_na_n - r'_na_n) = \\ (r_1 - r'_1)a_1 + (r_2 - r'_2)a_2 + \cdots + (r_n - r'_n)a_n \in I.\end{aligned}$$

If $r_1a_1 + r_2a_2 + \cdots + r_na_n \in I$ and $r \in R$,

$$\begin{aligned}r(r_1a_1 + r_2a_2 + \cdots + r_na_n) = (r_1a_1 + r_2a_2 + \cdots + r_na_n)r = \\ (rr_1)a_1 + (rr_2)a_2 + 1 \cdots + (rr_n)a_n \in I.\end{aligned}$$

Therefore I is an ideal by Theorem 14.1. □

(6) Let $\mathbb{Z}[x]$ be the ring of all polynomials with integer coefficients and let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant term. Then

$$I = \langle x, 2\rangle$$

is an ideal of $\mathbb{Z}[x]$.

PROOF.

[To show $I = \langle x, 2\rangle$.]

If $f(x) \in \langle x, 2\rangle$, $f(x) = xg(x) + 2h(x)$ where $g(x), h(x) \in R$. Then

$$f(0) = 0 \cdot g(0) + 2 \cdot h(0) = 2h(0),$$

so $f(x) \in I$. Also, if $f(x) \in I$,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + 2k = \\ x(a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots a_1) + 2k \in \langle x, 2\rangle.$$

Thus, by mutual inclusion, $I = \langle x, 2\rangle$.

[Show I is an ideal.] Suppose $k(x) \in \mathbb{Z}[x]$ and $f(x) = xg(x) + 2h(x) \in I$. Then

$$p(x) = f(x)k(x) = k(x)f(x) = xk(x)g(x) + 2k(x)h(x) \in I.$$

Also, if $f(x) = xf_1(x) + 2f_2(x)$ and $g(x) = f(x) = xg_1(x) + 2g_2(x)$,

$$f(x) - g(x) = x\big((f_1(x) - g_1(x)\big) + 2\big((f_2(x) - g_2(x)\big) \in I,$$

so I is an ideal by Theorem 14.1. □

(7) Let R be the ring of all real-valued functions of a real variable. Let S be the subset of all differentiable functions (this means for $f \in S$, $f'(x)$ is defined for all real x. S is <u>not</u> an ideal of R.

Let $f(x) = 1 \in S$ and let $g(x) = \operatorname{sgn} x = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$.

$h(x) = g(x)f(x) = \operatorname{sgn} x \notin S$. Thus S is not an ideal, but is a subring of R.

Factor Rings

THEOREM (14.2 — Existence of Factor Rings). *Let R be a ring and A a subring of R. The set of cosets $\{r+A|r \in R\}$ is a ring under the operations*

$$(s + A) + (t + A) = s + t + A \text{ and } (s + A)(t + A) = st + A \iff$$

A is an ideal of R.

[In this case , we say R/A is a factor ring of R.]

PROOF.

We know the set of cosets form a group under addition. If our multiplication is well-defined, i.e., multiplication is a binary operation, it is clear that the multiplication is associative and distributive over addition.

[To show multiplication is well-defined $\iff$ A is an ideal of R.]

($\Longleftarrow$) Suppose A is an ideal of R and let $s + A = s' + A$ and $t + A = t' + A$. Now $s = s' + a$ and $t = t$" $+ b$ where $a, b \in A$. Then

$$st = (s' + a)(t' + b) = s't' + s'b + at' + ab \Longrightarrow$$
$$st + A = s't' + s'b + at' + ab + A = s't' + A$$

since $s'b + at' + ab \in A$. Thus multiplication is well-defined.

($\Longrightarrow$) (using contrapositive) Suppose A is a subring of R that is not an ideal. then $\exists\ a \in A$ and $r \in R \ni- ar \notin A$ or $ra \notin A$. WLOG, assume $ar \notin A$. Consider $a + A = 0 + A$ and $r + A$.

$$(a + A)(r + A) = ar + A, \text{ but } (0 + A)(r + A) = 0 \cdot r + A = A \neq ar + A,$$

so multiplication is not well-defined and R/A is not a ring. □

EXAMPLE.

(1) $\mathbb{Z}/5\mathbb{Z} = \{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$ is a factor ring since $5\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

$$(3+5\mathbb{Z}) + (4+5\mathbb{Z}) = 7+5\mathbb{Z} = 2+5+5\mathbb{Z} = 2+5\mathbb{Z}$$

and

$$(3+5\mathbb{Z})(4+5\mathbb{Z}) = 12+5\mathbb{Z} = 2+10+5\mathbb{Z} = 2+5\mathbb{Z}.$$

We have essentially modular 5 arithmetic.

(2) $3\mathbb{Z}/9\mathbb{Z} = \{0+9\mathbb{Z}, 3+9\mathbb{Z}, 6+9\mathbb{Z}\}$is a factor ring since $9\mathbb{Z}$ is an ideal of $3\mathbb{Z}$, the arithmetic essentially modulo 9.

$$(6+9\mathbb{Z}) + (6+9\mathbb{Z}) = 12+9\mathbb{Z} = 3+9+9\mathbb{Z} = 3+9\mathbb{Z}$$

and

$$(6+9\mathbb{Z})(6+9\mathbb{Z}) = 36+9\mathbb{Z} = 9\mathbb{Z}.$$

(3) Let $R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \middle| a_i \in \mathbb{Z} \right\}$ and I be the subring of R consisting of matrices with even entries. I is an ideal of R.

PROOF.

Clearly, subtraction is closed in I. So let $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in R$ and

$\begin{bmatrix} 2b_1 & 2b_2 \\ 2b_3 & a_4 \end{bmatrix} = 2\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \in I$. Then

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} (2) \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = 2\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \right) \in I$$

and

$$\left(2\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \right) \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = 2\left(\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \right) \in I,$$

so I is an ideal. □

What is $|R/I|$?

SOLUTION.

Every member of R can be written in the form $\begin{bmatrix} 2a_1 + r_1 & 2a_2 + r_2 \\ 2a_3 + r_3 & 2a_4 + r_4 \end{bmatrix}$ where $a_i \in \mathbb{Z}$ and $r_i \in \{0, 1\}$. But

$$\begin{bmatrix} 2a_1 + r_1 & 2a_2 + r_2 \\ 2a_3 + r_3 & 2a_4 + r_4 \end{bmatrix} + I = \begin{bmatrix} 2a_1 & 2a_2 \\ 2a_3 & 2a_4 \end{bmatrix} + \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I.$$

Thus there are 2^4 choices for $\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}$ or 16 choices for the lements of R/I. □

EXAMPLE. Consider $R = \mathbb{Z}[i]/\langle 2 - i \rangle$, the factor ring of the Gaussian integers over $\langle 2 - i \rangle$. What are its elements?

For $r \in R$, $r = a + bi + \langle 2 - i \rangle$ as a start. Now $2 - i + \langle 2 - i \rangle = 0 + \langle 2 - i \rangle$, so we can consider $2 - i = 0 \bmod \langle 2 - i \rangle$ or $i = 2$. Then, as an example,

$$3 + 4i + \langle 2 - i \rangle = 3 + 8 + \langle 2 - i \rangle = 11 + \langle 2 - i \rangle.$$

Similarly, for all $r \in R$, $r = a + \langle 2 - i \rangle$ where $a \in \mathbb{Z}$.

Next, we also have, for $i = 2$, $i^2 = 4$ or $-1 = 4$ or $0 = 5$. Thus

$$7+6i+\langle 2-i \rangle = 7+12+\langle 2-i \rangle = 19+\langle 2-i \rangle = 4+5\cdot 3+\langle 2-i \rangle = 4+\langle 2-i \rangle.$$

It follows that

$$\{0 + \langle 2 - i \rangle, 1 + \langle 2 - i \rangle, 2 + \langle 2 - i \rangle, 3 + \langle 2 - i \rangle, 4 + \langle 2 - i \rangle\}.$$

Are any of these the same?

$$5(1 + \langle 2 - i \rangle) = 5 + \langle 2 - i \rangle = 0 + \langle 2 - i \rangle$$

so $|1 + \langle 2 - i \rangle|$ is 1 or 5. If $|1 + \langle 2 - i \rangle| = 1$, then

$$1 + \langle 2 - i \rangle = 0 + \langle 2 - i \rangle \Longrightarrow 1 \in \langle 2 - i \rangle \text{ or } 1 = (2 - i)(a + bi)$$

where $a+bi \in \mathbb{Z}[i]$. Then $2a+b+(-a+2b)i = 1$ or $2a+b = 1$ or $-a+2b = 0$. Then $5b = 1 \Longrightarrow b = \dfrac{1}{5}$, a contradiction. Thus $|1 + \langle 2 - i \rangle| = 5$ and $|R| = 5$.

EXAMPLE. Let $\mathbb{R}[x]$ be the ring of polynomials with real coefficients and $\langle x^2+1\rangle$ the principal ideal generated by x^2+1. Then

$$\langle x^2+1\rangle = \{f(x)(x^2+1)|f(x) \in \mathbb{R}[x]\}.$$

Now

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle|g(x) \in \mathbb{R}[x]\},$$

and (using the division algorithm for real polynomials),

$$g(x) = q(x)(x^2+1)+r(x)$$

where $r(x) = 0$ or the degree of $r(x)$ is less than 2, the degree of x^2+1.

Thus $r(x) = ax+b$ where $a, b \in R$. Thus $g(x) = q(x)(x^2+1)+ax+b$ and

$$g(x)+\langle x^2+1\rangle = ax+b+q(x)(x^2+1)+\langle x^2+1\rangle = ax+b+\langle x^2+1\rangle,$$

so

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{ax+b+\langle x^2+1\rangle|a, b \in \mathbb{R}\}.$$

How to multiply in $\mathbb{R}[x]/\langle x^2+1\rangle$?

Since $x^2+1+\langle x^2+1\rangle = 0+\langle x^2+1\rangle$, $x^2+1 = 0 \bmod x^2+1$ or $x^2 = -1$. Thus

$$(2x+3+\langle x^2+1\rangle)(5x-2+\langle x^2+1\rangle) =$$
$$10x^2+11x-6+\langle x^2+1\rangle = 11x-16+\langle x^2+1\rangle.$$

Note that, with x playing the role of i, this ring is isomorphic to the complex numbers.

Prime Ideals and Maximal Ideals

DEFINITION (Prime Ideal, Maximal Ideal). A prime ideal A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ implies $a \in A$ or $b \in A$. A maximal ideal A of R is a proper ideal of R if, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

EXAMPLE. Consider the ring $\mathbb{Z}$.

$\{0\}$ is a prime ideal of $\mathbb{Z}$. If $ab \in A$, then $ab = 0 \implies a = 0$ or $b = 0$ since $\mathbb{Z}$ is an integral domain $\implies a \in \{0\}$ or $b \in \{0\}$.

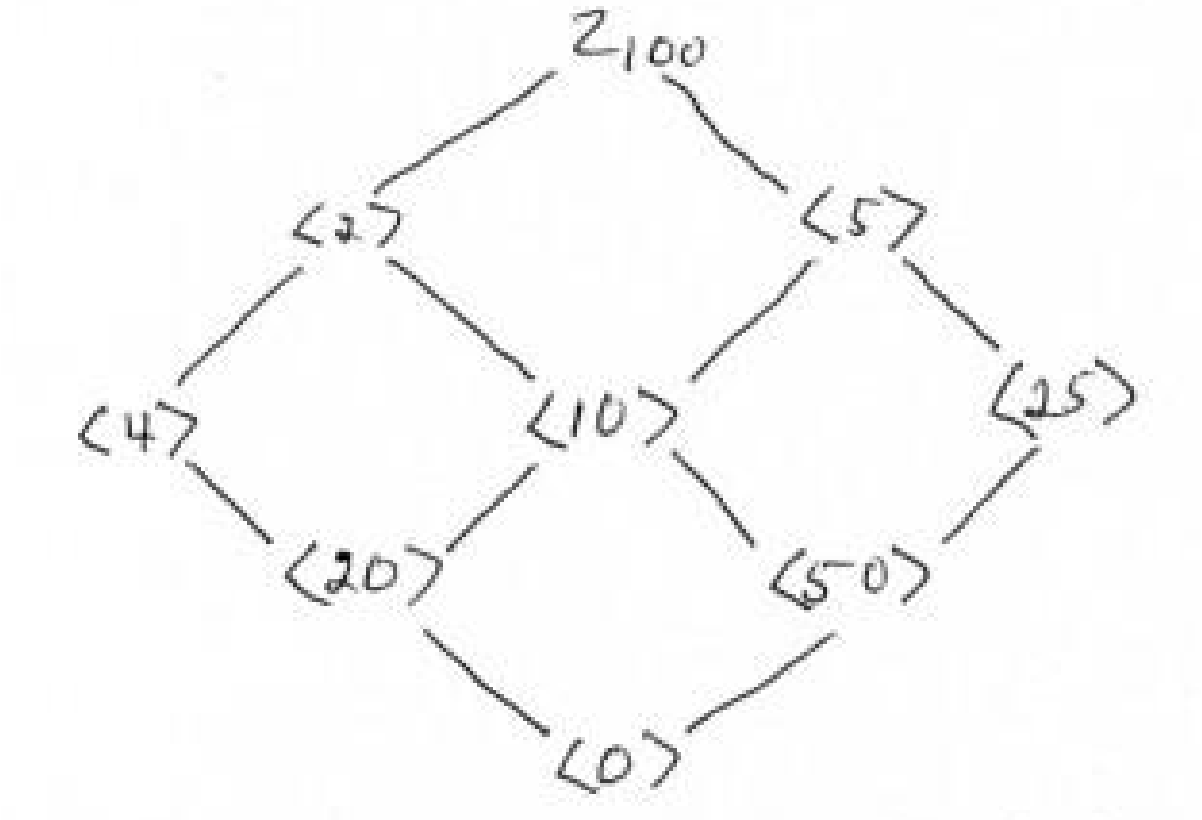
For $n > 1$, $n\mathbb{Z}$ is a prime ideal $\iff$ n is prime.

PROOF.

($\Longleftarrow$) Suppose n is prime. Recalling $\langle n \rangle = n\mathbb{Z}$, suppose $a, b \in \mathbb{Z}$ with $ab \in n$. Then $n|ab \implies$ (Euclid's Lemma) $n|a$ or $n|b \implies a \in \langle n \rangle$ or $b \in \langle n \rangle$. Thus $\langle n \rangle$ is prime.

($\Longrightarrow$) (by contrapositive) Suppose n is not prime. Then $n = st$ where $s < n$ or $t < n$. We have $st \in \langle n \rangle$, but $s \notin \langle n \rangle$ and $t \notin \langle n \rangle$, so $\langle n \rangle$ is not prime. $\square$

EXAMPLE. Consider the lattice of ideals of $\mathbb{Z}_{100}$.



The diagram shows that $\langle 2 \rangle$ and $\langle 5 \rangle$ are the maximal ideals.

PROBLEM (Page 275 # 15). If A is an ideal of a ring R and $1 \in A$, then $A = R$.

PROOF. Let $r \in R$. Then $r = r \cdot 1 \in A$. □

EXAMPLE. $\langle x^2 + 1 \rangle$ is a maximal ideal of $\mathbb{R}[x]$.

PROOF.

Suppose A is an ideal of $\mathbb{R}[x]$ and $\langle x^2 + 1 \rangle \subsetneqq A$,

[To show $\exists\ c \in \mathbb{R}, c \neq 0$, with $c \in A$.] Let $f(x) \in A, f(x) \notin \langle x^2 + 1 \rangle$. Then

$$f(x) = q(x)(x^2 + 1) + r(x)$$

where $r(x) \neq 0$ and $\deg r(x) < 2$. Then $r(x) = ax + b$ where a and b are not both 0, and

$$ax + b = r(x) = f(x) - q(x)(x^2 + 1) \in A.$$

Thus

$$a^2x^2 - b^2 = (ax + b)(ax - b) \in A, \text{ and } a^2(x^2 + 1) \in A$$

since $\langle x^2 + 1 \rangle \subseteq A$. Then

$$0 \neq a^2 + b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A.$$

Let $c = a^2 + b^2$. Since $c \in A$, $c \in \mathbb{R}[x] \Longrightarrow \dfrac{1}{c} \in \mathbb{R}[x]$, so $1 = \dfrac{1}{c} \cdot c \in A$. By Page 275 # 15, $A = \mathbb{R}[x]$, and so $\langle x^2 + 1 \rangle$ is a maximal ideal of $\mathbb{R}[x]$. □

EXAMPLE. $\langle x^2 + 1 \rangle$ is not prime in $\mathbb{Z}_2[x]$, since it contains

$$(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1,$$

but does not contain $x + 1$.

PROBLEM (Page 275 # 26). If R is a commutative ring with unity and A is a proper ideal of R, then R/A is a commutative ring with unity.

PROOF.

Note that

$$(b+A)(c+A) = bc+A = cb+A = (c+A)(b+A).$$

Thus R/A is commutative. Also, if 1 is the unit of R, $1+A$ is the unit of R/A. □

THEOREM (14.3 — R/A is an Integral Domain $\iff$ A is Prime). *Let R be a commutative ring with identity and let A be an ideal of R. Then R/A is an integral domain $\iff$ A is prime.*

PROOF.

($\Longrightarrow$) Suppose R/A is an integral domain and $ab \in A$. Then

$(a+A)(b+A) = ab+A = A \Longrightarrow a+A = A$ or $b+A = A \Longrightarrow a \in A$ or $b \in A$.

Thus A is prime.

($\Longleftarrow$) Note that R/A is a commutative ring with unity for any proper ideal A from Pge 275 # 26. Suppose A is prime and

$$(a+A)(b+A) = ab+A = 0+A = A.$$

Then $ab \in A \Longrightarrow a \in A$ or $b \in A$ since A is prime. Thus

$a+A = A$ or $b+A = A \Longrightarrow R/A$ has no zero-divisors and is thus an integral domain. □

PROBLEM (Page 275 # 25). Let R be a commutative ring with unity and let A be an ideal of R. If $b \in R$ and$B = \{br + a | r \in R, a \in A\}$, then B is an ideal of R.

PROOF.

For $br_1 + a_1, br_2 + a_2 \in B$ and and $r, r' \in R$,

$$(br_1 + a_1) - (br_2 + a_2) = b(r_1 - r_2) + (a_1 - a_2) \in B$$

and

$$r'(br + a) = b(r'r) + r'a \in B.$$

Thus B is an ideal by the ideal test. □

THEOREM (14.4 — R/A is a Field $\iff$ A is maximal). *Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field $\iff$ A is maximal.*

PROOF.

($\Longrightarrow$) Suppose R/A is a field and B is an ideal of R with $A \subsetneqq B$. Let $b \in B$, $b \notin A$. Then $b + A \neq A$, so $\exists\ c \in A \ni (b + A)(c + A) = 1 + A$, the multiplicative identity of R/A. Since $b \in B$, $bc \in B$. Because

$$1 + A = (b + A)(c + A) = bc + A,$$

$1 - bc \in A \subsetneqq B$. Thus $1 = (1 - bc) + bc) \in B$. By Page 275 # 15, $B = R$, so A is maximal.

($\Longleftarrow$) Suppose A is maximal and let $b \in R$, $b \notin A$.

[To show $b + A$ has a multiplicative inverse.]

Consider $B = \{br + a | r \in R, a \in A\}$. B is an ideal of R by Page 275 #25, and $A \subsetneqq B$ Since A is maximal, $B = R$. Thus $1 \in B$, say $1 = bc + a'$ where $a' \in A$. Then

$$1 + A = bc + a' + A = bc + A = (b + A)(c + A).$$

Thus R/A is a field. □

COROLLARY. *A maximal ideal is a prime ideal.*