3.15 Lecture 18: Principal ideals

Let R be a commutative ring and let $p \in R$.

- The element p is **prime** if p satisfies $p \neq 0$ and $pR \neq R$ and

$$\text{if } a, b \in R \text{ and } ab \in pR \text{ then } a \in pR \text{ or } b \in pR.$$

- The element p is **irreducible** if there do not exist $a, b \in R$ such that

$$p = ab \text{ and } a \notin R^\times \text{ and } b \notin R^\times.$$

In other words, an element $p \in R$ is prime if the principal ideal pR is a prime ideal.

HW: Let $R = \mathbb{Z}[x]$. The element x is irreducible and xR is a maximal principal ideal but xR is not a maximal ideal since $R \supsetneq 7R + xR \supsetneq xR$. The element x is also prime since $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$ which is an integral domain.

HW:. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}$. Define $N(a + b\sqrt{-5}) = a^2 + 5b^2$ so that if $x, y \in R$ then $N(xy) = N(x)N(y)$. The element $3 \in R$ is irreducible since $N(3) = 9$. The element 3 is not prime since 3 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ but 3 does not divide $1 + \sqrt{-5}$ and 3 does not divide $1 - \sqrt{-5}$.

Let

$$\mathcal{S}_0^R = \{\text{ideals of } R\} \qquad \text{and} \qquad \mathcal{P}_0^R = \{\text{principal ideals of } R\}$$

partially ordered by inclusion.

Proposition 3.71. *Let $\mathbb{A}$ be an integral domain.*

$$\begin{array}{ccc} \mathbb{A}/\mathbb{A}^\times & \longleftrightarrow & \mathcal{P}_0^R \\ d\mathbb{A}^\times & \longmapsto & d\mathbb{A} \end{array} \qquad \text{is a bijection.}$$

(b) Let $d \in \mathbb{A}$. Then d is irreducible if and only if $d\mathbb{A}$ is a maximal principal ideal of $\mathbb{A}$.

(c) Let $d \in \mathbb{A}$. If d is prime then d is irreducible.

(d) Let $d \in \mathbb{A}$. If $\mathcal{P}_{[0,R]}$ satisfies ACC and $d \neq 0$ and $d \notin \mathbb{A}^\times$ then there exist $k \in \mathbb{Z}_{>0}$ and irreducible $p_1, \ldots, p_k \in R$ such that $a = p_1 \cdots p_k$.

Proposition 3.72. *Let $\mathbb{A}$ be a PID.*

(a) Let $d \in \mathbb{A}$. Then d is prime if and only if d is irreducible.

(b) The poset $\mathcal{P}_{[0,\mathbb{A}]}$ of principal ideals of $\mathbb{A}$ satisfies ACC.

3.15.1 Some proofs

Proposition 3.73. *Let $\mathbb{A}$ be an integral domain.*

$$\begin{array}{ccc} \mathbb{A}/\mathbb{A}^\times & \longleftrightarrow & \mathcal{P}_0^R \\ d\mathbb{A}^\times & \longmapsto & d\mathbb{A} \end{array} \quad \textit{is a bijection.}$$

(b) Let $d \in \mathbb{A}$. Then d is irreducible if and only if $d\mathbb{A}$ is a maximal principal ideal of $\mathbb{A}$.

(c) Let $d \in \mathbb{A}$. If d is prime then d is irreducible.

(d) Let $d \in \mathbb{A}$. If $\mathcal{P}_{[0,R]}$ satisfies ACC and $d \neq 0$ and $d \notin \mathbb{A}^\times$ then there exist $k \in \mathbb{Z}_{>0}$ and irreducible $p_1, \ldots, p_k \in R$ such that $a = p_1 \cdots p_k$.

Proof.
To show: (aa) If $x, y \in \mathbb{A}$ and $x\mathbb{A} = y\mathbb{A}$ then there exists $u \in \mathbb{A}^\times$ such that $x = yu$.
(ab) If there exists $u \in \mathbb{A}^\times$ such that $x = yu$ then $x\mathbb{A} = y\mathbb{A}$.
(ba) If $d \in \mathbb{A}$ and d is irreducible then $d\mathbb{A}$ is a maximal principal ideal of $\mathbb{A}$.
(bb) If $d \in \mathbb{A}$ and $d\mathbb{A}$ is a maximal principal ideal of R then d is irreducible.

(aa) Assume $x, y \in \mathbb{A}$ and $x\mathbb{A} = y\mathbb{A}$.
Since $x \in y\mathbb{A}$ then there exists $v \in \mathbb{A}$ such that $x = yv$.
Since $y \in x\mathbb{A}$ then there exists $u \in \mathbb{A}$ such that $y = xu$.
So $x = yv = xuv$.
Using that $\mathbb{A}$ is an integral domain then the cancellation law gives that $uv = 1$.
So $u \in \mathbb{A}^\times$.

(ab) Assume that there exists $u \in \mathbb{A}^\times$ such that $x = yu$.
Then $x\mathbb{A} = yu\mathbb{A} \subseteq y\mathbb{A}$ and $y\mathbb{A} = xu^{-1}\mathbb{A} \subseteq x\mathbb{A}$.
So $x\mathbb{A} = y\mathbb{A}$.

(ba) Assume $d\mathbb{A}$ is not a maximal principal ideal.
Then there exists a principal ideal $g\mathbb{A}$ such that $d\mathbb{A} \subsetneq g\mathbb{A} \subsetneq \mathbb{A}$.
So $d = gh$ and $g \notin \mathbb{A}^\times$ and $h \notin \mathbb{A}^\times$.
So d is reducible.

(bb) Assume that d is reducible.
Then there exist $g, h \in \mathbb{A}$ such that $d = gh$ and $g, h \notin \mathbb{A}^\times$.
So $d\mathbb{A} \subsetneq g\mathbb{A} \subsetneq \mathbb{A}$.
So $d\mathbb{A}$ is not a maximal principal ideal.

(c) Assume that $d \in \mathbb{A}$ and d is prime.
To show: d is irreducible.
To show: If $d = ab$ then $a \in \mathbb{A}^\times$ or $b \in \mathbb{A}^\times$.
Assume $d = ab$. Then $ab \in d\mathbb{A}$.
Since d is prime then $a \in d\mathbb{A}$ or $b \in d\mathbb{A}$.
Case 1: $a \in d\mathbb{A}$.
Since $a \in d\mathbb{A}$ then there exists $r \in \mathbb{A}$ such that $a = dr$.
So $d = ab = drb$.
By the cancellation law, then $rb = 1$ and $b \in \mathbb{A}^\times$.
Case 2: $b \in d\mathbb{A}$.
Since $b \in d\mathbb{A}$ then there exists $s \in \mathbb{A}$ such that $b = ds$.
So $d = ab = das$.

By the cancellation law, then $as = 1$ and $a \in \mathbb{A}^\times$.

So d is irreducible.

(d) To show: If there exists $m \in R$ with $m \neq 0$ and $m \notin R^\times$ that does not have a finite factorization into irreducible then $\mathcal{P}_0^R$ does not satisfy ACC.

Assume that there exists $m \in R$ with $m \neq 0$ and $m \notin R^\times$ that does not have a finite factorization into irreducible elements.

Since m is not irreducible then there exist $a, b \in R$ such that $a, b \notin R^\times$ and $m = ab$.

Since m does not have a finite irreducible factorization then at least one of a and b does not have an irreducible factorization.

So there exists $m_1 \in R$ such that

$$mR \subsetneq m_1R \subsetneq R \qquad \text{and } m_1 \text{ does not have a finite irreducible factorization.}$$

Repeating the process with m_1, there exists $m_2 \in R$ such that

$$mR \subsetneq m_1R \subsetneq m_2R \subsetneq R \qquad \text{and } m_2 \text{ does not have a finite irreducible factorization.}$$

In this way $mR \subsetneq m_1R \subsetneq m_2R \subsetneq \cdots$ is a non-finite increasing chain in $\mathcal{P}_0^R$.

So $\mathcal{P}_0^R$ does not satisfy ACC.

□

Proposition 3.74. *Let $\mathbb{A}$ be a PID.*

(a) Let $d \in \mathbb{A}$. Then d is prime if and only if d is irreducible.

(b) The poset $\mathcal{P}_{[0,\mathbb{A}]}$ of principal ideals of $\mathbb{A}$ satisfies ACC.

Proof.

(a) $\Rightarrow$: Assume that $d \in \mathbb{A}$ and d is prime.

To show: d is irreducible.

To show: If $d = ab$ then $a \in \mathbb{A}^\times$ or $b \in \mathbb{A}^\times$.

Assume $d = ab$. Then $ab \in d\mathbb{A}$.

Since d is prime then $a \in d\mathbb{A}$ or $b \in d\mathbb{A}$.

Case 1: $a \in d\mathbb{A}$.

Since $a \in d\mathbb{A}$ then there exists $r \in \mathbb{A}$ such that $a = dr$.
So $d = ab = drb$.
By the cancellation law, then $rb = 1$ and $b \in \mathbb{A}^\times$.

Case 2: $b \in d\mathbb{A}$.

Since $b \in d\mathbb{A}$ then there exists $s \in \mathbb{A}$ such that $b = ds$.
So $d = ab = das$.
By the cancellation law, then $as = 1$ and $a \in \mathbb{A}^\times$.

So d is irreducible.

(a) $\Leftarrow$: Assume that $d \in \mathbb{A}$ and d is irreducible.

So $d\mathbb{A}$ is a maximal principal ideal.

Since $\mathbb{A}$ is a PID then $\mathcal{S}_{[0,R]} = \mathcal{P}_{[0,R]}$ and $d\mathbb{A}$ is a maximal ideal.

Since $d\mathbb{A}$ is a maximal ideal then $d\mathbb{A}$ is a prime ideal.

So $d \in \mathbb{A}$ is prime.

(b) Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in $\mathbb{A}$.

To show: There exists $k \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{>k}$ then $I_n = I_k$.

Let

$$I_{\mathrm{un}} = \bigcup_{j \in \mathbb{Z}_{>0}} I_j.$$

Then I_{un} is an ideal of $\mathbb{A}$.

Since $\mathbb{A}$ is a PID then there exists $d \in \mathbb{A}$ such that $I_{\mathrm{un}} = d\mathbb{A}$.

To show: There exists $k \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{>k}$ then $I_n = I_k$.

Let $k \in \mathbb{Z}_{>0}$ such that $d \in I_k$.

To show: If $n \in \mathbb{Z}_{>k}$ then $I_n = I_k$.

Assume $n \in \mathbb{Z}_{>k}$. Then

$$I_k \subseteq I_n \subseteq I_{\mathrm{un}} = d\mathbb{A} \subseteq I_k.$$

So $I_n = I_k$.

So $\mathbb{A}$ satisfies ACC.

$\square$