Introduction to Rings and Modules

Lecture 7, Monday May 8 2023

Ari Feiglin

Proposition 7.0.1:

If R is an integral domain and $a, b \in R$, then $(a) = (b)$ if and only if there exists an invertible u such that $a = bu$.

Proof:

If there does exist such a u, then $a = bu$ so $a \in (b)$ and so $(a) \subseteq (b)$, and $b = au^{-1}$ so $(a) = (b)$. If $(a) = (b)$ then $a = bu$ and $b = av$, so $a = avu$ so $a(1 - vu) = 0$, and since R is an integral domain, either $a = 0$ or $1 - vu = 0$. If $a = 0$ this is trivial, otherwise $vu = 1$ and so v and u are invertible as required. ■

Definition 7.0.2:

If $a, b \in R$ and there exists an invertible u such that $a = bu$ then a and b are considered **friends**.

Thus in an integral domain, $(a) = (b)$ if and only if a and b are friends.

Proposition 7.0.3:

If R is Artinian, every quotient ring of R's is Artinian.

Proof:

Suppose $I \trianglelefteq R$ is an ideal. If there exist a descending chain of ideals in ${}^{R}\!/_{I}$, then it is of the form

$$ {}^{J_1}\!\Big/_{I} \supset {}^{J_2}\!\Big/_{I} \supseteq \cdots $$

where $J_i \trianglelefteq R$ by the correspondence theorem. Thus the J_is form a descending chain of ideals in R, and must stabilize. And therefore so must their quotients. ■

Proposition 7.0.4:

If R is an Artinian integral domain, R is a field.

Proof:

Let $0 \neq a \in R$, notice that for every n, $a^{n+1} = a \cdot a^n \in (a^n)$, so $(a^{n+1}) \subseteq (a^n)$. So we have a decreasing chain of ideals $(a) \supseteq (a^2) \supseteq \cdots$. Since R is artinian, there exists an N such that $(a^N) = (a^{N+1}) = \cdots$. This is only if there exists an invertible element u such that $a^N u = a^{N+1} = a^N a$. Thus $a^N(a - u) = 0$ and so $a^N = 0$ or $a = u$, since R is an integral domain and $a \neq 0$, $a^N \neq 0$, so $a = u$. And since u is invertible, a is invertible. ■

Proposition 7.0.5:

If R is a commutative Artinian ring, $\dim R = 0$.

Proof:

Suppose $\dim R > 0$, then there exist at least two prime ideals P_0 and P_1 such that $P_0 \subset P_1$. Since P_0 is a prime ideal, ${}^{R}\!/_{P_0}$ is an integral domain, and since R is Artinian so is the quotient ring. Therefore ${}^{R}\!/_{P_0}$ is a field, therefore P_0 is maximal. But this is a contradiction since it is properly contained within P_1. ■

Definition 7.0.6:

Let R be a commutative ring, and $p \neq 0$ a non-invertible element. Then p is **irreducible** if for every decomposition $p = ab$, a or b is invertible.

Proposition 7.0.7:

Let R be a principal ideal domain, let $p \in R$ be irreducible. Thus (p) is maximal and therefore prime.

Proof:

Suppose I is a proper ideal such that $(p) \subseteq I$. Then since R is a PID, $I = (a)$, so $p \in (p) \subseteq (a)$. Therefore $p = ab$. Since p is irreducible, a or b is invertible. Since I is proper, it cannot contain invertible elements, so b must be invertible. Therefore $a = pb^{-1}$ and so $(p) = (a) = I$, so (p) is indeed maximal. ■

Recall that I is maximal in a commutative ring R if and only if ${}^{R}\!/_{I}$ is a field. And J is a prime ideal in a commutative ring R if and only if ${}^{R}\!/_{J}$ is an integral domain. Since fields are integral domains, that means I is a prime ideal.

Example 7.0.8:

This is not true if R isn't a PID. Take $R = \mathbb{Q} + x\mathbb{R}[x] \subseteq \mathbb{R}[x]$, the ring of all real polynomials with rational free coefficients. $x \in \mathbb{R}[x]$ is irreducible since if $x = fg$, then either $\deg f$ or $\deg g$ is 0 (since $\deg(fg) = \deg f + \deg g$), and so f or g is invertible. But (x) is not prime in R since

$$(\sqrt{2}x)(\sqrt{2}x) = 2x^2 \in (x)$$

but $\sqrt{2}x \notin (x)$ so $(\sqrt{2}x) \nsubseteq (x)$.

Definition 7.0.9:

Let R be a PID, R is called a **unique factorization domain** (UFD) if for every $0 \neq a \in R$ non-invertible, there exists a factorization

$$a = p_1 p_2 \cdots p_r$$

such that every p_i is irreducible. And if $a = q_1 q_2 \cdots q_s$ then $r = s$ and there exists a permutation σ such that p_i and $q_{\sigma(i)}$ are friends for every i.

Definition 7.0.10:

Let R be a commutative ring, and $a, b \in R$, then we say $a|b$ (a divides b) if there exists a $q \in R$ such that $b = qa$. (If R is not commutative there is the notion of left and right divisors.)

Proposition 7.0.11:

Every PID is a unique factorization domain.

Proof:

Let $0 \neq a \in R$ not invertible. We claim there exists a irreducible p such that $p|a$. Suppose that there doesn't, then a is not irreducible (a is reducable) since a divides itself. Therefore there exists a factorization $a = b_1 c_1$ such that b_1 and c_1 are not invertible. And so b_1 is decomposable (since $b_1|a$), so there exists a factorization $b_1 = b_2 c_2$ where b_2 and c_2 are not invertible. Since $a = b_2 c_2 c_1$, so $b_2|a$ and so b_2 is decomposable. So we can continue recursively to get b_ns and c_ns where

$$b_n = b_{n+1} c_{n+1}$$

and b_n and c_n are not invertible and decomposable. So

$$(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \cdots$$

Since R is a PID, it is Noetherian, so at some point $(b_N) = (b_{N+1})$. So b_N and b_{N+1} are friends, so there exists a u such that $b_N = b_{N+1}u = b_{N+1}c_{N+1}$, so

$$b_{N+1}(u - c_{N+1}) = 0 \implies u = c_{N+1}$$

so c_{N+1} is invertible, which is a contradiction.
We now claim that a has a factorization into irreducible p_is. By above, we know that there exists a $p_1 \in R$ irreducible such that $p_1|a$, so $a = p_1b_1$. If b_1 is invertible then p_1 and a are friends and so if $a = xy$ then $p_1 = xyb_1^{-1}$ so x is invertible or yb_1^{-1} is invertible, and so x or y is invertible. So if b_1 is invertible, a is irreducible and so $a = a$ is a factorization.
Otherwise $0 \neq b_1$ is not invertible and so there exists a irreducible p_2 such that $p_2|b_1$ and so $b_1 = p_2b_2$. If b_2 is invertible, then b_1 is irreducible so $a = p_1b_1$ is a factorization. Otherwise, we continue recursively. If at any point we have that b_n is invertible, we have finished. Otherwise we have a sequence of p_n irreducible and b_n invertible such that $b_n = p_{n+1}b_{n+1}$, and so $(b_n) \subseteq (b_{n+1})$. So we have an ascending chain of ideals, and since R is Noetherian, at some point $(b_N) = (b_{N+1})$ and so $b_N = b_{N+1}u = b_{N+1}p_{N+1}$, and so $u = p_{N+1}$ as R is an integral domain. But p_{N+1} is irreducible and therefore not invertible, in contradiction. So every $0 \neq a \in R$ non-invertible has a factorization.
Now we must show that this factorization is unique. Suppose that

$$a = p_1p_2 \cdots p_n = q_1q_2 \cdots q_m$$

where q_i and p_i are irreducible. Then we have that

$$a = q_1 \cdots q_m \in (p_1)$$

and since p_1 is irreducible, (p_1) is prime so there exists an i such that $q_i \in (p_1)$. We can assume $i = 1$ since we don't care about the order of the factorization. Therefore $(q_1) \subseteq (p_1)$ and since q_1 is irreducible, (q_1) is maximal, so $(q_1) = (p_1)$ and therefore q_1 and p_1 are friends. So there exists an invertible u_1 such that $q_1 = u_1p_1$ and so

$$p_1(p_2 \cdots p_n - u_1q_2 \cdots q_m) = 0$$

and so $p_2 \cdots p_n = u_1q_2 \cdots q_m$. Again there must be a q_i or a u_1q_i in (p_2) (since if u_2 in (p_2) then p_2 is invertible), since $(u_1q_i) = (q_i)$ since u_1 is invertible, we have that $(q_i) = (p_i)$ for the same reason as before. We can also assume $i = 2$ and so p_2 and q_2 are friends and $q_2 = u_2p_2$, and we can continue inductively. Thus for every p_i there exists a q_i which it is friends with. So $n \leq m$, if $n < m$ then at the end of the induction we get that

$$1 = u_1 \cdots u_n \cdot q_{n+1} \cdots q_m$$

and so $q_{n+1} \cdots q_m$ is invertible, so $(q_{n+1} \cdots q_m) = R$ but this is contained in (q_m) so $(q_m) = R$ so q_m is invertible which is a contradiction since it is irreducible. So $n = m$ and the factorization is unique. ∎