MATH 171 FALL 2008: LECTURE 17

DAGAN KARP

1. Primes and Irreducibles

We begin with a generalization of the notion of prime in integral domains.

Definition 1. *Let R be an integral domain, and let $r \in R$ be a nonzero non-unit. Then r is* irreducible *if $r = a \cdot b$, for some $a, b \in R$, implies a or b is a unit in R. Otherwise r is* reducible.

Example 2. *Prime numbers in $\mathbb{Z}$ are irreducible. Indeed, if $p = ab$ for a prime p and integers a, b, then both a and b divide p, which implies $(a, b) \in \{(1, p), (p, 1)\}$. Therefore either a or b is a unit in $\mathbb{Z}$ and p is irreducible.*

Definition 3. *A nonzero element p of an integral domain R is* prime *if the ideal (p) generated by p is a prime ideal.*

Remark 4. In other words, the nonzero p is prime in R if and only if $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$, i.e. ab is a multiple of p implies a is a multiple of p or b is a multiple of p, i.e. $p|ab$ implies $p|a$ or $p|b$.

Proposition 5. *In an integral domain, every prime element is irreducible.*

Proof. Let R be an integral domain, and let $p \in R$ be prime. Suppose $p = ab$ for some $a, b \in R$. Then $ab \in (p)$. Therefore $a \in (p)$ or $b \in (p)$. If $a \in (p)$, then there exists $r \in R$ such that $a = pr$. Thus

$$p = ab = prb,$$

and hence $p(1 - rb) = 0$. But $p \neq 0$ by assumption since p is prime. Further R is an integral domain, so $1 - rb = 0$. Therefore b is a unit. Similarly, $b \in (p)$ implies that a is a unit. Thus $p = ab$ implies that a or b is a unit. □

Remark 6. It is not the case that irreducible implies prime in integral domains. For example, consider the domain $R = \mathbb{Z}\sqrt{-5}$. We claim that $3 \in R$ is irreducible but not prime. That 3 is irreducible is elementary but tedious and I'm not going to include the details here. (Assume that there are integers a, b, c, d such that $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Then $ad + bc = 0$ and $3 = ac - 5bd \ldots$) However the ideal (3) is not prime in R. Indeed, note that

$$(2 - \sqrt{-5})(2 + \sqrt{-5}) = 4 + 5 = 9 \in (3).$$

But no multiple of 3 is equal to $2 - \sqrt{-5}$ or $2 + \sqrt{-5}$ in R. Hence (3) is not a prime ideal.

Proposition 7. *In a principal ideal domain, every irreducible element is prime.*

Date: November 2, 2008.

Proof. Let $r \in R$ be an irreducible element in a PID. We must show that r is prime, i.e. that (r) is a prime ideal. In fact, we prove the stronger statement: (r) is maximal.

Suppose $I \subseteq R$ is an ideal containing (r),

$$(r) \subseteq I \subseteq R.$$

Since R is a PID, $I = (s)$ for some $s \in R$. Thus $(r) \subseteq (s)$. Hence there exists $a \in R$ such that

$$r = sa.$$

But r is irreducible. Thus s or a is a unit in R. If s is a unit, then $I = (s) = R$. Otherwise a is a unit, and $(r) = (s) = I$. Therefore (r) is a maximal ideal. □

Combining the above, we have the following.

Corollary 8. *In a PID, a nonzero element is prime if and only if it is irreducible.*

2. Unique Factorization Domains

In the integers, prime numbers play a basic role in decomposition of integers, namely prime factorizations. With our new general notions of prime and irreducible, we can generalize this notion to rings other than integers.

Definition 9. *An integral domain R is a* unique factorization domain *if every nonzero non-unit element $r \in R$ can be written as a finite product of irreducibles p_i of R,*

$$r = p_1 p_2 \cdots p_n.$$

Further, this decomposition is required to be unique up to units: If

$$r = q_1 q_2 \cdots q_m,$$

where q_i is irreducible for all i, then $m = n$ and there is a permutation $\sigma \in S_n$ and units $u_1, \ldots, u_n$ such that

$$q_{\sigma(i)} = p_i u_i.$$

Example 10. *UFD's and non UFD's.*

1. *A field F is a UFD trivially. Indeed, the set of all nonzero non-unit elements of F is the empty set.*
2. *The integral domain $\mathbb{Z}\sqrt{-5}$ is not a UFD since*

   $$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

   are two distinct irreducible decompositions of 6.

From this last example, we see that all UFD's are integral domains, but not all integral domains are UFD's. Similarly, it turns out that all UFD's are PID's, but not all PID's are UFD's. In order to prove such a theorem, we need several preliminary results.

Proposition 11. *Let $p \in R$ be an element of a UFD. Then p is prime if and only if p is irreducible.*

Proof. Since R is an integral domain, prime implies irreducible. We must show the converse. So, suppose p is irreducible. We will show that p is prime. Suppose $ab \in (p)$ for some $a, b \in R$. Then there exists $c \in R$ such that $ab = pc$. Choose some irreducible decomposition of a and b,

$$a = s_1 s_2 \cdots s_n \qquad\qquad b = t_1 t_2 \cdots t_m,$$

where s_i and t_j are irreducible for all i, j. Then we have

$$ab = pc = s_1 s_2 \cdots s_n t_1 t_2 \cdots t_m.$$

Since p is irreducible, the uniqueness of the above irreducible decomposition of the element $ab \in R$ implies that, up to a unit, p is equal to a factor of a or b. Without loss of generality, we have

$$s_i = pu$$

for some i and unit $u \in R$. But then $p|s_i$ and hence $p|a$. □

Proposition 12. *Let $0 \neq a, b \in R$ be two nonzero elements of a UFD. Suppose*

$$a = up_i^{a_i} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = vp_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where $p_1, \ldots, p_n$ are distinct primes, u and v are units and the integer exponents are nonnegative $a_i, b_i \geqslant 0$. Then

$$d = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

is the greatest common divisor of a and b.

Proof. First note that indeed d is a common divisor of a and b, since the exponent of each prime factor of d is not larger than the corresponding power in a and b. Let d' be any other common divisor, and consider its prime factorization

$$d' = q_1^{c_1} q_2^{c_2} \cdots q_m^{c_m}.$$

Then each q_i divides d' and hence divides a and b. Thus there is some prime p_j such that q_i divides p_j by the previous proposition. Therefore

$$q_1 q_2 \cdots q_m | p_1 p_2 \cdots p_n.$$

Also, the exponents of d' must be less than or equal to the exponents of d. Therefore $d'|d$.

Theorem 13. *Principal ideal domains are unique factorization domains.*

Proof. Let R be a PID, and let $a \in R$. We wish to show that a has an irreducible decomposition, unique up to units. If a is irreducible, then we are done. Otherwise, there exist nonzero non-units a_1, a_2 such that

$$a = a_1 \cdot a_2.$$

If a_1, a_2 are irreducible, then we are done. Otherwise one is reducible; suppose it is a_1. Then there exist two nonzero non-units a_{11}, a_{12} such that

$$a_1 = a_{11} \cdot a_{12} \qquad\qquad a = a_{11} a_{12} a_2.$$

We may repeat this process, continuing to decompose all reducible factors of a. Of course, we need this process to terminate in order to express a as a *finite* product of irreducible elements.

Note that the above factorization algorithm produces a strictly ascending chain of ideals

$$(a) \subsetneqq (a_1) \subsetneqq (a_{11}) \subsetneqq \cdots \subsetneqq R.$$

We have shown that only finite ascending chains of ideals exist in PID's. Therefore this chain is finite. Hence the above factorization is finite.

We now must show that this decomposition is unique up to units. This is a straightforward application of induction. □

Corollary 14 (Fundamental Theorem of Arithmetic)**.** *The integers are a UFD.*

Proof. The integers are a Euclidean domain, hence a PID, hence a UFD.