MATH 171 FALL 2008: LECTURE 16

DAGAN KARP

1. Principal Ideal Domain

Proposition 1. *Every ideal in a Euclidean domain is principal.*

Proof. Let $I \subseteq R$ be an ideal of a Euclidean domain with norm N. If $I = \{0\}$, then the result holds. Otherwise, consider the set

$$\{N(a) : 0 \neq a \in I\} \subseteq \mathbb{N} \cup \{0\}.$$

As a subset of nonnegative integers, this set has a minimum. Let $d \in I$ be any nonzero element of minimum norm. We claim that $I = (d)$. First, since $d \in I$, we have $(d) \subseteq I$. Now, let $a \in I$. The by the division algorithm, there exist $q, r \in R$ such that

$$a = qd + r,$$

where $r = 0$ or $N(r) < N(d)$. But we may write $r = a - qd \in I$. Therefore $N(r) \geqslant N(d)$ as d is of minimum norm. Therefore $r = 0$, and thus $a = qd$ and $a \in (d)$. Therefore $I \subseteq (d)$. □

Definition 2. *A* principal ideal domain *is an integral domain in which every ideal is principal.*

Example 3. *Some basic examples:*

1. $\mathbb{Z}[x]$ *is not a principal ideal, as we have shown directly* $(2, x)$ *is not principal.*
2. $\mathbb{Z}$ *is a PID, as every ideal is a subring, and hence as a set a subgroup, and hence cyclic, as* $\mathbb{Z}$ *is cyclic.*

Proposition 4. *Let* R *be a PID, and let* $I \subseteq R$ *be a nonzero ideal. If* I *is prime, then* I *is maximal.*

Proof. Suppose that J is an ideal and

$$I \subseteq J \subseteq R.$$

We show that $I = J$ or $J = R$. First, since R is a PID, I and J must be principal, and there exist a and b in R such that $I = (a)$ and $J = (b)$. Since $I \subset J$, we have $(a) \subseteq (b)$ and hence $a \in (b)$. So there exists an element $x \in R$ such that

$$a = bx.$$

But then $bx \in (a)$. Now (a) is prime, and thus $b \in (a)$ or $x \in (a)$.

Date: October 29, 2008.

If $b \in (a)$, then $(b) \subseteq (a)$, i.e. $J \subseteq I$ and hence $J = I$. Otherwise $x \in (a)$. So there exists $y \in R$ such that $x = ya$. Thus

$$a = bx = bya,$$

and so $a(1 - by) = 0$. But $a \neq 0$ since I is nonzero. Hence $1 - by = 0$ and $by = 1$. Thus b is a unit and $J = (b) = R$. $\square$

Corollary 5. *Let R be a commutative ring. If $R[x]$ is a PID, then R is a field.*

Proof. Since $R \subseteq R[x]$ is a subring, R is also an integral domain. Note that the principal ideal (x) is nonzero and is prime, since

$$R[x]/(x) \cong R,$$

and R is an integral domain. By the above Proposition, (x) is thus a maximal ideal. But then

$$R[x]/(x) \cong R$$

is a field. $\square$

Proposition 6. *(Ascending chain condition) In a PID, any strictly ascending chain of ideals*

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \cdots$$

must be finite in length.

Proof. Let I be the union of all ideals of the PID R in this chain

$$I = \bigcup_{n \in \mathbb{N}} I_n.$$

First note that I is an ideal of R. It's elementary to see that I is a subring of R. If $a \in I$, then there is some n such that $a \in I_n$. Then $ra \in I_n \subset I$ for any $r \in R$. Thus I is indeed an ideal.

Thus I is Principal, as R is a PID. Thus there is an element $b \in R$ such that $I = (b)$. Then there is some m such that $b \in I_m$. Thus $(b) \subseteq I_m$. But for any i,

$$I_i \subseteq I = (b) \subseteq I_m.$$

Therefore I_m is the last member of the chain. $\square$

Exercise. (8.1)# 4 Let R be a Euclidean domain.

(1) Prove that if $(a, b) = 1$, and $a|bc$, then $a|c$. More generally, let a, b be nonzero. If $a|bc$, then $a/(a, b)$ divides c.
(2) Let $0 \neq a, b \in \mathbb{Z}$ and $N \in \mathbb{Z}$. Suppose there are integers x_0, y_0 such that

$$ax_0 + by_0 = N.$$

Show that if x and y are any other solutions,

$$ax + by = N$$

then there exists an integer m such that

$$x = x_0 + m\frac{b}{(a,b)} \qquad\qquad y = y_0 - m\frac{a}{(a,b)}.$$

Moreover, any such x, y are indeed solutions for any integer m. [*Hint: show that* $a(x - x_0) = b(y - y_0)$ *and use (1).*]

Exercise. Can you show directly the ideal $(3, 2+\sqrt{-5})$ is not principal in the ring $\mathbb{Z}[\sqrt{-5}]$?