Lecture 17 (Ascending Chain Conditions. Euclidean Domains and the Gaussian Integers)

Finitely Generated Ideals and the Ascending Chain Condition

Definition 17.1 (Finitely Generated Ideals) An ideal I of a ring commutative ring R is said to be finitely generated if there are element $a_1, a_2, \ldots, a_n \in R$ such that

$$I = a_1R + a_2 + \cdots + a_nR = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \,|\, r_1, r_2 \ldots, r_n \in R\}.$$

We then say $a_1, a_2, \ldots, a_n$ generate I.
Note if R has an identity then each $a_i \in I$.

Example A principle ideal is an ideal with a single generator. In a P.I.D. every ideal is finitely generated.

Theorem 17.2 Let R be a commutative ring with identity R. Then R satisfies the ascending chain condition for ideals if and only if every ideal of R is finitely generated.

Proof Suppose every ideal of R is finitely generated. Let

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

is an ascending chain of ideals. We show it stabilises.
The union $I = \cup I_n$ of the ascending chain is an ideal of R. So there are elements $a_1, a_2, \ldots, a_n \in I$ which generate I. Hence for each i, $a_i \in I_{N_i}$ for some N_i. If we put $N = \max\{N_1, \ldots N_n\}$ then for each i, $a_i \in I_{N_i} \subseteq I_N \Rightarrow a_iR \subseteq I_N$. Hence

$$I = a_1R + \cdots + a_nR \subseteq I_N \subseteq I_{N+1} \subseteq I_{N+2} \cdots \subseteq I.$$

We deduce $I_N = I_{N+1} = I_{N+2} = \ldots = I$.
We now show if R has a non-finitely generated ideal then R has an ascending chain of ideals which does not stabilise. Suppose I is a non-finitely generated ideal of R. Let a_1 be any element of I. Set $I_1 = a_1R$. Then $I_1 \subsetneqq I$. Choose $a_2 \in I \setminus I_2$. Set $I_2 = a_1R + a_2R$. Then $I_1 \subsetneqq I_2 \subsetneqq I$. Now choose $a_3 \in I \setminus I_2$ etc. In this way we can construct a strictly ascending chain of ideals of R. $\square$

Euclidean Domains

Definition 17.3 (Euclidean Domains An integral domain R is a Euclidean domain if there is a function $d : R \setminus \{0\} \to \mathbb{N}$ such that

(E1) For all non-zero $a, b \in R$, $d(a) \leq d(ab)$.

(E2) For all non-zero $a, b \in R$ there exist $q, r \in R$ such that $a = qb+r$ where either $r = 0$ or $d(r) < d(b)$.

The integers $\mathbb{Z}$ are a Euclidean ring with $d(a) = |a|$. Any polynomial ring $F[x]$ over a field F is Euclidean with $d(f) = \deg f$.

Theorem 17.4 A Euclidean domain is a principle ideal domain.

Proof Main idea: show that if I is a non-zero ideal and a in I has $d(a)$ minimal then $I = aR$.

Corollary In a Euclidean domain every element is a product of primes, and this product is unique up to associates and ordering of the factors.

Lemma 17.5 Let R be Euclidean and a, u nonzero elements of R. Then $d(au) = d(a)$ if and only if u is a unit.
In particular $u \in R$ is a unit if and only if $d(u) = d(1)$.

Proof Consider the non-zero ideal $I = aR$. Because $d(a) \leq d(ax)$ for any $x \neq 0$ in R the d value of a is minimal for the d-values of elements in aR. Suppose u is a unit. Then $auR = I$. So $d(au)$ is minimal for the d-value of elements in I. Hence $d(au) = d(a)$. Now suppose $d(au) = d(a)$. Then by the main idea of the proof above, $auR = aR$. Hence u is a unit.

□

Corollary An element $u \in R$ is a unit if and only if $d(u) = d(1)$. □

The Gaussian Integers

Definition 17.6 (The Gaussian Integers) The Gaussian integers are the subset $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ of $\mathbb{C}$ the complex numbers with integer coefficients. They form a subring of $\mathbb{C}$.

Definition 17.7 For $z = x + iy \in \mathbb{C}$, $Nz = z\bar{z} = x^2 + y^2 \in R$ is called the norm of z.

Simple Properties of the Norm For all $z, w \in \mathbb{C}$,

N1. $N(zw) = NzNw$;

N2. $N\bar{z} = Nz$;

N3. $Nz \geq 0$ with equality if and only if $z = 0$.

N4. $|z| = \sqrt{Nz}$.