MATH 171: WORKSHEET 8

DAGAN KARP

1. Unique Factorization Domains

Recall that in a PID, an ideal is maximal if and only if it is prime. (In any integral domain, maximal implies prime.)

Proposition 1. *Let R be a PID, and let $I \subseteq R$ be a nonzero ideal. If I is prime, then I is maximal.*

Corollary 2. *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. □

Proposition 3. *(Ascending chain condition) In a PID, any strictly ascending chain of ideals*

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots$$

must be finite in length.

Remark 4. Note that this is equivalent to the following. For any ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

there exists an $N \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$ for $n \geqslant N$.

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. □

Definition 5. *A* Noetherian Ring *is a commutative ring with identity that satisfies the ascending chain condition.*

Theorem 6. *Let* R *be a commutative ring with identity. Then* R *is Noetherian if and only if every ideal of* R *is finitely generated.*

Proof. Suppose R is Noetherian. Let I be an ideal of R. If $I = \{0\}$ then it is finitely generated. Otherwise, let $0 \neq a_1 \in I$. If $(a_1) = I$ we are done. Otherwise, choose $0 \neq a_2 \in I \setminus (a_1)$. If $(a_1, a_2) = I$ we are done. Iterate this process, and define

$$I_n = (a_1, a_2, \ldots, a_n).$$

Then

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

is a strictly ascending chain of ideals. Since R is Noetherian, there is an $n \in \mathbb{N}$ such that $I_m \subseteq I_n$ for all $m \in \mathbb{N}$. Therefore

$$I = (a_1, \ldots, a_n)$$

and I is finitely generated.

Conversely, suppose that every ideal of R is finitely generated. We prove that R is Noetherian. Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals. Then let

$$I = \bigcup_{k=1}^{\infty} I_k.$$

Then I is finitely generated, and hence there exists $a_1, \ldots a_n \in R$ such that $I = (a_1, \ldots, a_n)$. But $a_i \in I$, hence there exists k_i such that $a_i \in I_{k_i}$ for each i. Let

$$N = \text{MAX}\{k_i : i = 1, \ldots, n\}.$$

Then $I = I_N$, and hence $I_n \subseteq I_N$ for all n. Thus R has no strictly ascending infinite chain of ideals, and R is Noetherian. □

Definition 7. *Let* R *be an integral domain. A nonzero element* $0 \neq p \in R$ *is* irreducible *if* $p = ab$ *implies* a *or* b *is a unit. We say* p *is* prime *if* $p|ab$ *implies* $p|a$ *or* $p|b$.

Remark 8. Note that both of these properties hold for prime numbers in the integers. So we have two generalizations of our notion of prime here.

Definition 9. *An integral domain* D *is said to be a* unique factorization domain *if every nonzero non-unit* $a \in D$ *may be written as a product of irreducible elements uniquely up to associates (units). In more detail, let* $0 \neq a \in D$ *not be a unit. Then there exist irreducible elements* $p_1, \ldots, p_n$ *in* D *such that*

$$a = p_1 \cdots p_n.$$

Moreover, if $a = q_1 q_2 \cdots q_m$ *for irreducible elements* $q_j \in D$*, then* $m = n$ *and there exists a permutation* $\sigma \in S_n$ *such that* p_1 *and* $q_{\sigma(i)}$ *are associates, i.e. there are units* u_i *such that*

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

Theorem 10. *Every PID is a UFD.*

Proof. Here's the idea. Let R be a PID and let $a \in R$ be a nonzero non-unit. We show that a can be factored. If a is irreducible, we are done. Otherwise,

$$a = a_1 b_1$$

where neither are units. Then $(a) \subsetneq (a_1)$. If a_1 is not irreducible, then $a_1 = a_2 b_2$ where neither are units. Continue to construct an ascending chain of ideals.