MATH H113: Honors Introduction to Abstract Algebra

2016-04-18

- gcd's
- P.I.D.'s

Skip universal side divisors (p. 277) and Dedekind-Hasse norms (p. 281 - 2)

Correction: Last time I mentioned Ex 8.4.14 (when showing that $F[x]$ is a Euclidean domain). That should have been 7.4.14.

Definition: Let R be a commutative ring, and let $a, b \in R$

a. We say $a \mid b$ (or a *divides* b or a is a *divisor* of b, or b is a *multiple* of a) if $ax = b$ for some $x \in R$.
b. A common divisor of a and b is an element $d \in R$ such that $d \mid a$ and $d \mid b$.
c. A *greatest common divisor* of a and b is an element $d \in R$ such that
    i. d is a common divisor of a and b, and
    ii. if d' is another common divisor of a and b, then $d' \mid d$

(common multiples and least common multiples are defined similarly, see the homework). Compare with the definition in $\mathbb{Z}$: i. There is no "$\leq$" in R (usually), so we don't require gcd's to be > 0. ii. w define $\gcd(0, 0)$ (it's 0)

Existence: there exists ring in which not all gcd's exist.
Uniqueness: **Lemma**: Let R be a commutative ring, and let $a, b \in R$. Then:

a. $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$
b. $d \in R$ is a common divisor of a and $b \iff (d) \supseteq (a, b)$.
c. $d \in R$ is a gcd of a and b if and only if (d) is the smallest principal ideal containing (a, b).

Proof: (a) and (b) should be easy exercises.
(c). d is a gcd $\iff$ d is a common divisor and d' a common divisor $\implies d' \mid d$
(a), (b) $\iff$ $(d) \supseteq (a, b)$ and if $(d') \supseteq (a, b)$ then $(d') \supseteq (d)$.
$\iff$ (d) is the smallest principal ideal containing (a, b).
Corollary: If both d and d' are gcd's of a and b, then $(d) = (d')$. Furthermore, if R is an integral domain, then $d = ud'$ for some unit $u \in R$.
Proof: first part: the smallest element of a poset is unique (if it exists).
The second part is then by Ex. 7.4.8 ($(d) = (d') \iff d = ud' forsomeunitu$)
Definition: Let R be a commutative ring with 1. Then elements $a, b \in R$ are *associates* if $a = ub$ for some unit u of R. This is an equivalence relation.

Examples: In $\mathbb{Z}$, a and b are associates $\iff a = \pm b$. In a Euclidean domain, a and b are associates $\iff a = b = 0$ or $b \neq 0$ and $\frac{a}{b}$ is a unit.
So, gcd's in an integral domain are unique up to associates.
So, for this definition of gcd, in $\mathbb{Z}$, gcd's are only unique up to sign.
But, in a Euclidean domain, we can still use the Euclidean algorithm to compute gcd's . (See homework.)
In a Euclidean domain, gcd's exist (to be proved shortly).

Principal Ideal Domains

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

Proposition: Let R be a Euclidean domain with (Euclidean) norm N. Let I be a non-zero ideal in R, and let d be a nonzero element of I having minimal norm (among nonzero elements of I).
Then $I = (d)$.
Proof: First of all d exists because the $\{N(d) : d \in I, d \neq \emptyset\}$ is a nonempty subset of $\mathbb{N}$, so it has a smallest element.
Then $(d) \subseteq I$ because $d \in I$.

On the other hand, let $a \in I$. Write $a = qd + r$ with $q, r \in R$ and ($r \neq 0$ or $N(r) < N(d)$). Then we must have $r = 0$ (otherwise, since $r = a - qd$ and $a, d \in I$, $r \in I$, and $r \neq 0$ with $N(r) < N(d)$, contradicting the choice of d). Then $a = qd$, so $a \in (d)$. This shows $I \subseteq (d)$. Therefore $I = (d)$.

Theorem: If R is a Euclidean domain, then R is a P.I.D.
Proof: Let R be a Euclidean domain, and let I be an ideal of R. If $I = 0$ then $I = (0)$ is principal. Otherwise $I \neq 0$, so $I = (d)$ for d as in the proposition.

Proposition: IN a P.I.D. (or a Euclidean domain) gcd's exist.
Proof: Let R be a $P.I.D.$ and let $a, b \in R$. Then $(a, b) = (d)$ for some $d \in R$. That shows that d is a gcd of a and b.

Examples:

1. $\mathbb{Z}$ is a P.I.D., so are all Euclidean domains
2. $\mathbb{R}[x, y]$ is not a P.I.D., because its ideal (x, y) is not principal. Therefore, it's not a Euclidea domain, either. However, $\gcd(x, y)$ exists ($= 1$, or any nonzero constant polynomial).

Proposition Let R be a P.I.D. and let $a, b \in R$. Then:

a. $\gcd(a, b)$ exists, and equals d for any d such that $(d) = (a, b)$.

b. FOr such d, $d = ax + by$ for some $a, b \in R$.

Proof:

a. Was already noted (if $(a, b) = (d)$ then (d) is the smallest principal ideal containing (a, b)).
b. With d as above, $d \in (a, b) = \{ax + by : x, y \in R\}$ The $=$ is true because any ideal containing a and b must also contain $ax + by$ $\forall x, y \in R$. So $(a, b) \supseteq \{ax+by : x, y \in R\}$. On the other hand, $a, b \in \{ax+by : x, y \in R\}$, and $\{ax + by : x, y \in R\}$ is an ideal in R.

Note: in $\mathbb{R}[x, y]$, you *can't* write $\gcd(x, y)$ as an R-linear combination of x and y.

Proposition: In a P.I.D., every nonzero prime ideal is a maximal ideal.
Proof: Let P be a nonzero prime ideal. Then $P = (p)$ for some $p \in R$, $p \neq 0$.
Let I be some ideal of R with $P \subseteq I \subseteq R$. We want to show that $I = P$ or $I = R$.
Then $I = (m)$.
Since $p \in P$ and $P \subseteq I$, $p \in I$, so $p = mx$ for some $x \in R$. Since P is prime and $mx \in P$, either $m \in P$ or $x \in P$.
If $m \in P$ then $(m) \subseteq P$, so $I \subseteq P$, $\therefore I = P$ because $I \supseteq P$.
If $x \in P$ then $x = ps$ for some $s \in R$, so $p = mx = mps$, $\therefore ms = 1$, so m is a unit and $(m) = R$. $\therefore I = P$ or $I = R$, so P is maximal.