Rutgers University: Algebra Written Qualifying Exam

January 2008: Day 2 Problem 7 Solution

Exercise. Let D be a principal ideal domain and let E be a commutative domain containing D as a subring (a commutative domain is also called an *integral domain*). Let $a, b \in D$ and suppose that $d \in D$ is a greatest common divisor of a and b in D. Prove that d is also a greatest common divisor of a and b in E.

Solution.

D is a **principal ideal domain**, so if I is an ideal
[i.e. $(I, +)$ a subgroup of $(D, +)$ and $ir \in I$ for all $i \in I$]
and $r \in D$] then $I = \langle g \rangle$ for some $g \in D$.

E is a **commutative domain**, so it is a commutative ring with no zero divisors.

Let d be a **gcd** of a and b in D. If $c \in D$ such that $c \mid a$ and $c \mid b$, then $c \mid d$

$\langle a, b \rangle$ is an ideal of D and $\gcd(a, b) = d$ in D
Since D is a PID,

$$\begin{array}{llll} & \langle a,b \rangle = \langle p \rangle & & \text{for some } p \in D \\ \Longrightarrow & a \in \langle p \rangle & \text{and} & b \in \langle p \rangle \\ \Longrightarrow & p \mid a & \text{and} & p \mid b \\ \Longrightarrow & p \mid d & & \text{since } d \text{ is the gcd of } a \text{ and } b \text{ in } D \end{array}$$

$$\begin{array}{lll} & \langle a,b \rangle = \langle p \rangle & \\ \Longrightarrow & p \in \langle a,b \rangle & \\ \Longrightarrow & p = ra + sb & \text{for some} r, s \in D \\ \Longrightarrow & d \mid p & \text{since } d \mid a \text{ and } d \mid b \end{array}$$

$$\text{Thus,} \quad d = p \qquad \text{since } d \mid p \text{ and } p \mid d$$

Thus, if D is a PID and the gcd of a and b in D is d, then $\langle a, b \rangle = \langle d \rangle$.

$$\begin{array}{lll} \gcd(a,b) = d & \Longleftrightarrow & \langle a,b \rangle = \langle d \rangle \\ & \Longleftrightarrow & \exists x, y, u, v \in D \text{ s.t. } \quad a = dx \\ & & \qquad b = dy, \text{ and} \\ & & \qquad au + bv = d \end{array}$$

Let $c \in E$ s.t. $c \mid a$ and $c \mid b$
Then $c \mid \underbrace{(au + bv)}_{=d}$ since $u, v \in D \subseteq E$.
So the gcd of a and b in E is d.