4/1/14

HW 4 due now.

Exam 2 on Thurs.

Today: Review

The main topic for the exam is

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

Definition: Let $R$ be a domain. We say that $R$ is Euclidean if there exists a function $\delta: R \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

- $a = qb + r$
- $r = 0$ or $\delta(r) < \delta(b)$.

Remarks:

- The $q, r$ need not be unique.
- The main examples are

$\mathbb{Z}$ with $\delta(n) = |n|$

$K[x]$ with $\delta(f) = \deg(f)$.

**Definition:** We say that $R$ is a PID if every ideal $I \subseteq R$ is principal, i.e., there exists $a \in R$ such that

$$I = (a) = \{ar : r \in R\}.$$

**Theorem:** Euclidean $\Rightarrow$ PID.

**Proof:** Let $(R, \delta)$ be Euclidean and consider any ideal $I \subseteq R$. If $I = (0)$ we're done, so suppose $I \neq (0)$ and choose $0 \neq b \in I$ with $\delta(b)$ minimal.

Then for any $a \in I$ we divide by $b$ to get

- $a = qb + r$
- $r = 0$ or $\delta(r) < \delta(b)$

Since $r = a - qb \in I$, $\delta(r) < \delta(b)$ is impossible. Hence $r = 0$ and we conclude that $I = (a)$. ///

**Definition:** We say that $R$ is a UFD if

(1) Every element can be factored into irreducibles, times a unit.
(2) Irreducible $\Rightarrow$ Prime.

In this case, suppose we have

$$u p_1 p_2 \cdots p_k = v q_1 q_2 \cdots q_\ell$$

with $u, v \in R^\times$ and the $p_i, q_j$ irreducible. Then

$$p_1 \mid q_1 q_2 \cdots q_\ell$$

since irreducible $\Rightarrow$ prime we have $p_1 \mid q_j$ for some $j$. WLOG assume that $p_1 \mid q_1$. Then since $q_1$ is irreducible we conclude that $q_1 = w p_1$ for some $w \in R^\times$. Since $R$ is a domain we can cancel to get

$$u p_2 p_3 \cdots p_k = (vw) q_2 q_3 \cdots q_\ell.$$

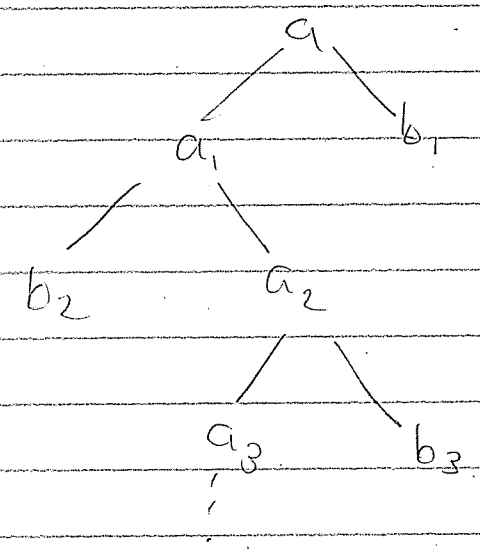
Continuing in this way we find that $k = \ell$ and

$$p_2 = q_2$$
$$\vdots$$
$$p_k = q_k.$$

So irreducible factorizations are unique.

**Theorem:** PID $\Rightarrow$ factorization Exists.

**Proof:** Let $R$ be a PID and consider nonunit, nonzero $a \in R$. Assume for contradiction that $a$ has NO factorization into irreducibles. Then the "factorization tree" of $a$ is not finite, so it has an infinite branch:




We obtain an infinite increasing chain of ideals

$$(a) < (a_1) < (a_2) < \cdots$$

Let $J := \bigcup_{i=1}^{\infty} (a_i)$. I claim that $J \in R$ is an ideal.

Indeed, given $x, y \in J$ and $r \in R$, $\exists\, m, n \in \mathbb{N}$ such that $x \in (a_m)$, $y \in (a_n)$. Let $N = \max\{m, n\}$ so that $x, y \in (a_N)$. Then since $(a_N)$ is an ideal we have

$$x - ry \in (a_N) \subseteq J. \qquad ///$$

Thus $J$ is an ideal. Since $R$ is a PID we have $J = (b)$ for some $b \in R$. Since $b \in J$, $\exists\, n \in \mathbb{N}$ such that $b \in (a_n)$. But then we have

$$J = (b) \subseteq (a_n) \subsetneq (a_{n+1}) \subseteq J.$$

Contradiction. ///

Theorem (Euclid's Lemma):

Irreducible $\Rightarrow$ Prime in a PID.

Proof: Let $R$ be a PID and let $p \in R$ be irreducible. We will show that $p$ is prime. So suppose that $\exists\, a, b \in R$ such that

$$p \mid ab \text{ (say } ab = pk) \text{ and } p \nmid a$$

We will show that $p \mid b$. Since $p \nmid a$ we get a strict inclusion of ideals.

$$(p) \subsetneq (a) + (p) \leq (1)$$

Since $R$ is a PID we have $(a) + (p) = (d)$. Then since $(p) < (d) \leq (1)$ and $p$ is irreducible we must have

$$(a) + (p) = (d) = 1.$$

Since $1 \in (a) + (p)$, $\exists\ x, y \in R$ such that

$$ax + py = 1$$

Multiply both sides by $b$ to get

$$abx + pby = b$$
$$pkx + pby = b$$
$$p(kx + by) = b.$$

Hence $p \mid b$. //

Corollary: PID $\Rightarrow$ UFD. //

## Application to Polynomials:

Let $L \supseteq K$ be a field extension and consider $\alpha \in L$. Then the function

$$\begin{aligned} ev_\alpha : K[x] &\longrightarrow L \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

is a ring homomorphism. Since $K[x]$ is Euclidean is a PID. Hence the kernel is generated by a single polynomial called the <u>minimal polynomial</u>

$$\ker(ev_\alpha) = (m_\alpha(x)) \leq K[x].$$

<u>Theorem</u>: If $m_\alpha(x) \neq 0$ then $m_\alpha(x)$ is irreducible.

<u>Proof</u>: Suppose for contradiction that

$$m_\alpha(x) = f(x)g(x)$$

for some $f, g \in K[x]$ with

$$\begin{aligned} 1 < \deg(f) < \deg(m_\alpha) \\ 1 < \deg(g) < \deg(m_\alpha). \end{aligned}$$

Evaluate at $\alpha$ to get

$$0 = m_\alpha(\alpha) = f(\alpha)g(\alpha).$$

Since $R$ is a domain this implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. WLOG suppose that $f(\alpha) = 0$, hence $f(x) \in (m_\alpha(x))$. Then $m_\alpha(x) \mid f(x)$ implies that

$$\deg(m_\alpha) \leq \deg(f).$$

Contradiction. ///

Corollary: If $m_\alpha(x)$ then

$$K[\alpha] := \mathrm{im}(ev_\alpha) = \{ f(\alpha) : f(x) \in K[x] \}$$

is a field.

Proof: By the First Isomorphism Theorem we have

$$K[\alpha] = \mathrm{im}(ev_\alpha) \cong \frac{K[x]}{\ker(ev_\alpha)} = \frac{K[x]}{(m_\alpha(x))}.$$

I claim that $(m_\alpha(x))$ is a maximal ideal. If not then there exists an ideal

$$(m_\alpha) < J < K[x].$$

Since $K[x]$ is a PID we have $J = (f)$ for some $f(x) \in K[x]$ and hence

$$(m_\alpha) < (f) < K[x].$$

But then $f$ is a proper divisor of $m_\alpha$, contradicting the fact that $m_\alpha$ is irreducible.

Finally by the Correspondence Theorem we have

$(m_\alpha)$ maximal
$\Rightarrow \mathcal{L}(K[x], (m_\alpha)) = \{K[x], (m_\alpha)\}$
$\Rightarrow \mathcal{L}(K[x]/(m_\alpha)) = \{K[x]/(m_\alpha), (0)\}$.
$\Rightarrow K[x]/(m_\alpha)$ is a field.
$\Rightarrow K[\alpha]$ is a field. ///