6/3/14

Review of 661/662

We have seen:

(1) Abstract Groups
(2) Groups Acting on Things

Today: Abstract Rings

We say $\varphi : R \to R'$ is a ring hom. if

- $\forall a, b \in R$, $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\forall a, b \in R$, $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_{R'}$

"subring $\equiv$ image of ring hom."

Proof: Easy

"ideal $\equiv$ kernel of ring hom"

Proof: kernel is an ideal. ✓.

Conversely, let $I \leq R$ be an ideal and consider the additive group R/I.

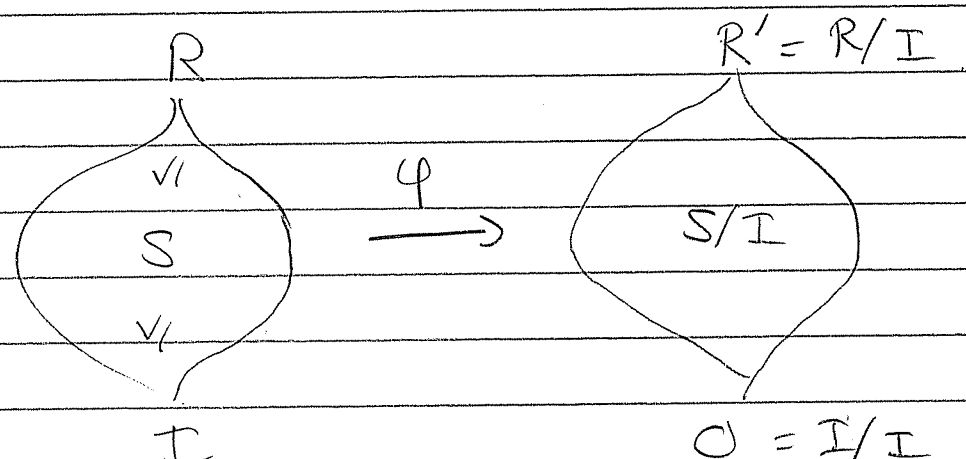
Because I is an ideal, the natural map

$$\varphi : R \twoheadrightarrow R/I$$
$$a \longmapsto a + I$$

defines a ring structure on R/I. Then φ is a ring hom with $I = \ker \varphi$. ///

☆ Correspondence Theorem for Rings:

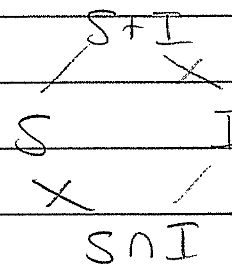
Let $\varphi : R \twoheadrightarrow R'$ be a surjective ring hom. with kernel $I \trianglelefteq R$. Then we have a ring isomorphism $R' \approx R/I$. This induces an isomorphism of lattices of ideals (and subrings):



There are various "isomorphism theorems" that are easy to prove.

<u>Example</u>: Let R be a ring with ideal $I \subseteq R$ and subring $S \subseteq R$. Prove that we have an isomorphism of rings

$$\frac{S}{S \cap I} \approx \frac{S+I}{I}$$



[Hint: Restrict $\varphi : R \to R/I$ to S.]

Ideals generalize to modules. We say M is an R-module if $(M, +, 0)$ is an abelian group with an R-action $R \times M \to M$ satisfying

- $r(x+y) = rx + ry$
- $(r+s)x = rx + sx$
- $(rs)x = r(sx)$
- $1x = x$

for all $r, s \in R$, $x, y \in M$.

We say $N \subseteq M$ is an R-submodule if

$\forall\, x, y \in N, r \in R, \quad x - ry \in N.$

We say $\varphi : M \to M'$ is an R-module hom
(R-linear map) if

$\forall\, x, y \in M, r \in R, \quad \varphi(x - ry) = \varphi(x) - r\varphi(y).$

Exercise: kernels and images are both R-submodules. There is no structural difference between them.

Warning: The structure of modules is very rich, as you know. It is the modern formalism of algebra.

Instead of pursuing category theory we go back to the beginning.

Let R be commutative with 1. We say R is Euclidean if $\exists$ size function $\sigma : R \setminus 0 \to \mathbb{N}$ such that $\forall\, a, b \in R$ with $b \neq 0$ $\exists\, q, r \in R$ such that

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

There are two examples:

- $\mathbb{Z}$ with $\delta(a) = |a|$
- $K[x]$ with $\delta(f) = \deg(f)$.

The attempt to pretend they are the same is called "algebraic geometry". It provides motivation for the mess we call "commutative algebra".

Theorem: Euclidean $\Longrightarrow$ PID.

Proof: let $I \leq R$ be an ideal and choose $0 \neq b \in I$ with $\delta(b)$ minimal (by well-ordering of $\mathbb{N}$). Then for any $a \in I$ divide to get

$$a = qb + r \text{ with } r = 0 \text{ or } \delta(r) < \delta(b).$$

Note that $r = a - qb \in I$. If $r \neq 0$ then $\delta(r) < \delta(b)$ is a contradiction. Hence $r = 0$ and we conclude that $I = (b)$. ///

Theorem: PID $\Rightarrow$ Noetherian

<u>Proof</u>: Suppose for contradiction we have a strict chain of ideals

$$J_1 < J_2 < J_3 < \cdots \leq R.$$

Since $J := \bigcup_i J_i$ is an ideal (Exercise) we have $J \leq (b)$ for some $b \in R$. Since $b \in J$ we have $b \in J_m$ for some $m \in \mathbb{N}$ and then

$$(b) \leq J_m \lneq J_{m+1} \leq J = (b).$$

Contradiction. //

<u>Def</u>: We say $p \in R$ is irreducible if

$$p = ab \implies a \text{ OR } b \text{ is a unit.}$$

We say $p \in R$ is prime if

$$p \mid ab \implies p \mid a \text{ OR } p \mid b.$$

Euclid's Lemma: In a PID we have

irreducible $\Rightarrow$ prime.

<u>Proof</u>: let $p \in R$ be irreducible and suppose that $p \mid ab$ (say $ab = pk$) and $p \nmid a$. Since $p \nmid a$ and since R is PID we have

$$(p) \subsetneq (a) + (p) = (d)$$

for some $d \in R$. Since p is irreducible this implies d is a unit, hence $(a)+(p) = (d) = R$. Since $1 \in (a)+(p)$ $\exists\, x, y \in R$ with

$$1 = ax + py.$$
$$b = abx + pby$$
$$b = pkx + pby$$
$$b = p(kx + by),$$

hence $p \mid b$ as desired. ///

So far we have not needed R to be a domain. Now we need it.

Theorem: PID $\Rightarrow$ UFD.

Proof: Given $a \in R$ use Noetherian property to write

$$a = p_1 p_2 \cdots p_k$$

with p_i irreducible. Suppose we also have

$$a = q_1 q_2 \cdots q_\ell$$

with q_j irreducible. Since $p_1 \mid q_1 q_2 \cdots q_\ell$ and p_1 is prime (Euclid), WLOG we have $p_1 \mid q_1$. Since q_1 is irred this implies $q_1 = p_1 u$ for some unit u.

Now use the fact that R is a domain to cancel:

$$p_2 p_3 \cdots p_k = u\, q_2 q_3 \cdots q_\ell .$$

We're done by induction. $\blacksquare$