Algebra I: Chinese Remainder Thm

Make shorter

Throughout: all rings are comm. w/ 1 ≠ 0.

Advertise topics course

Direct prod. of rings $R_1, \dots, R_n$.

As an ab. gp, is the direct prod. of $(R_1,+), \dots, (R_n,+)$.

Ring mult. component-wise too.

Eg: $R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R\}$,

$$(r_1,r_2)+(s_1,s_2) = (r_1+s_1, r_2+s_2)$$
$$(r_1,r_2)\cdot(s_1,s_2) = (r_1 \cdot s_1, r_2 \cdot s_2).$$

pre-write on board

Inherits ring structure from $R_1, \dots, R_n$ trivially.

Note: $\varphi: R \to R_1 \times R_2 \cdots \times R_n$ is a hom.

$\iff$ each $\varphi_i = \pi_i \circ \varphi : R \to R_i$ is a hom.

$\pi_i : R_1 \times \cdots \times R_n \to R_i$

$(r_1, \dots, r_n) \mapsto r_i$. projection.

Recall: integers m, n are coprime

$\iff$ def $\gcd(m,n) = 1 \iff 1 = mx + ny$ for some $x, y \in \mathbb{Z}$

$\iff 1 \in (m,n) \iff (m,n) = \mathbb{Z}$.

(get a unit) (ideal)

That is,
m, n determine ideals $m\mathbb{Z}, n\mathbb{Z}$, and this is $\iff$ to

$$m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}.$$

More generally:

Def^n: Ideals A, B in R are comaximal if $A + B = R$.

Recall: Product of ideals:

$AB = \{$finite sums of the form $x \cdot y,\ x \in A, y \in B\}$.

If $A = (a)$, $B = (b)$, this is simply $AB = (ab)$.

ab: $xy = ra\,rb = rr'(ab)$

More generally,

$A_1 \cdots A_k$ = ideal of all finite sums of elts.

$x_1 \cdots x_k \quad x_i \in A_i\ \forall i$.

If $A_i = (a_i)$, then $A_1 \cdots A_k = (a_1 \cdots a_k)$.

Th^m (Chinese Remainder Theorem)

$A_1, \ldots, A_k$ ideals in R. The map.

$$R \longrightarrow R/A_1 \times \cdots \times R/A_k$$
$$r \longmapsto (r + A_1, \ldots, r + A_k)$$

is a ring. hom. with kernel

$$A_1 \cap A_2 \cap \cdots \cap A_k.$$

If for each $i, j \in \{1, \ldots, k\}$ with $i \neq j$.

A_i, A_j are comaximal, then this map is surjective

and $A_1 \cap \cdots A_k = A_1 \cdots A_k$. Thus, in this case,

$$R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k.$$

Pf: Use induction

Base case: $k=2$:

Let $A = A_1$, $B = A_2$.

$\varphi: R \to R/A \times R/B$

$r \mapsto (r \bmod A, r \bmod B)$.

By the note above, this is a ring hom.

as its compositions with projections to R/A, R/B are.

$\varphi_1 : R \to R/A$

$r \mapsto r \bmod A$

$\varphi_2 : R \to R/B$

$r \mapsto r \bmod B$.

which are the canonical ring quotient projection maps.

$\ker(\varphi) = \{r \mid r \bmod A = 0 \bmod A,\ r \bmod B = 0 \bmod B\}$

$= \{r \mid r \in A, r \in B\} = A \cap B$.

Now suppose A, B are comaximal.

Since $A + B = R$, $\exists x \in A, y \in B$ s.t. $x + y = 1$.

Then, $\varphi(x) = (0,1)$, and $\varphi(y) = (1,0)$, as, e.g.

$x \in A$ and $x = 1 - y \in 1 + B$, so $x = 0 \bmod A$.
$x = 1 \bmod B$.

To show φ is surjective, let $(r_1 \bmod A, r_2 \bmod B)$

be an arb. elt. in $R/A \times R/B$.

a preimage under φ is then $r_2 x + r_1 y$ since

$\varphi(r_2 x + r_1 y) = \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y)$.

$= (r_2 \bmod A, r_2 \bmod B)(0,1)$

$+ (r_1 \bmod A, r_1 \bmod B)(1,0)$

$= (0, r_2 \bmod B) + (r_1 \bmod A, 0) = (r_1 \bmod A, r_2 \bmod B)$.

Thus, ψ is surjective

We now want: $AB = A \cap B$.

We always have $AB \subseteq A \cap B$, as A, B are ideals

Since A, B are comax $\Leftrightarrow$ $x+y=1$ for some x, y, for any $c \in A \cap B$, we have.

$c = c \cdot 1 = cx + cy \in AB \Rightarrow A \cap B \subseteq AB$.

Thus $AB = A \cap B$. (think about analogues in $\mathbb{Z}$).

The result when $k=2$ follows from the 1st Iso. Thm

Inductive step: ~~Suppose~~

Follows from case $k=2$ using

$A = A_1$, and $B = A_2 \cdots A_k$.

~~Observe~~ show $A_1, A_2 \cdots A_k$ are comax $\Leftrightarrow$.

By hypothesis, for each $i \in \{2, 3, \ldots, k\}$ $\exists$ s.t. $x_i \in A_1, y_i \in A_i$

$A_1 \cdot x_i + y_i = 1$.

Now $x_i + y_i \equiv y_i \bmod A_1$, and so

$1 = (x_2 + y_2) \cdots (x_k + y_k)$ is in $A_1 + (A_2 \cdots A_k)$.

Special (famous) case: m, n coprime integers.

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

This gives us our kinds of classifications of cyclic gps we studied before

This says that solving

$x \equiv a \bmod m$

$x \equiv b \bmod n$

simultaneously is always possible, and is unique mod $m \cdot n$.

(studied in China)

More generally, if $n_1, \ldots, n_k \in \mathbb{N}$,

are pairwise coprime, & we set $n_1 \cdot \cdots \cdot n_k = N$,

then given any integers $a_1, \ldots, a_k$, then $\exists\, x \in \mathbb{Z}$ s.t.

$x \equiv a_1 \bmod n_1$

$x \equiv a_2 \bmod n_2$

$\vdots$

$x \equiv a_k \bmod n_k$.

and any two sol^{ns} x are $\equiv \bmod N$.

In terms of rings,

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Corollary: The units gps on both sides are $\cong$!

The units in a direct product ring are the direct product of unit gps. Thus,

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^\times.$$

We can thus take any $n \in \mathbb{N}$, and factorize into a powers of distinct primes:

$n = p_1^{a_1} \cdots p_k^{a_k}$. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$$

and

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$

Cor: $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$.

$\varphi(n)$ = Euler φ fn $= |(\mathbb{Z}/n\mathbb{Z})^\times|$.

That is, φ is multiplicative:

$\varphi(m)\varphi(n) = \varphi(mn)$ when $(m,n) = 1$

(but not completely multiplicative, as not always $=$).

Thus φ is determined by its values on prime powers.

But $\varphi(p^a) = p^a - p^{a-1}$ as the set of #s $1, \ldots, p^a$ coprime to p^a are those coprime to p, so just the set of non-multiples of p. There are p^{a-1} #s $p = 1 \cdot p, 2 \cdot p, \ldots, p^{a-1} \cdot p = p^a$.

Other apps: Lagrange interpolation (closely related)

(extra time) use norm map to show $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

(6)