NOTES ON RINGS, MATH 369.101

More on Rings

So multiplicative cancellation in rings does not generally work. In addition, there might be a non-zero element which can be raised to a power to get zero – a **nilpotent** element.

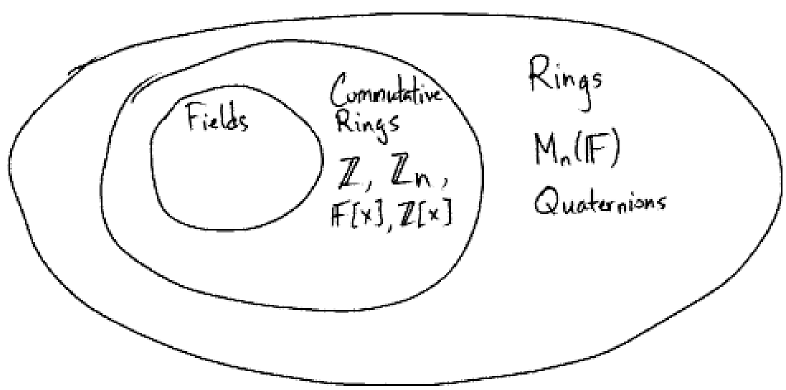
Examples:

(1) In $\mathbb{Z}_8$: $[2]^3 = [2][2][2] = [8] \equiv [0]$.

(2) In $M_2(\mathbb{F})$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(3) In $M_3(\mathbb{F})$, $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Recall, we have the following.



Note that for any $f(x) \in \mathbb{F}[x]$, the set of congruence classes $\mathbb{F}[x]/\langle f(x)\rangle$ is a commutative ring.

Date: Oct. 12 – Oct. 19.

[If you look at the proof of Theorem 4.3.6, none of the axioms that are used for a commutative ring required that $f(x)$ is irreducible. That was used to get multiplicative inverses.]

Relaxing coefficients. Let R be any ring.

Then $R[x]$, polynomials with coefficients in R, is a ring. This ring is commutative if and only if R is commutative.

You can also have $M_n(R)$, matrices with entries in R, and this with matrix addition/multiplication is a ring.

One has to be careful about inverses. For example, $\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$ has an inverse in $M_2(\mathbb{Q})$ but as a matrix in $M_2(\mathbb{Z})$ it does not have an inverse.

The direct sum. For any rings R and S.

$R \oplus S$, as a set, is the ordered pairs:

$$R \oplus S = \{(r,s) \big| r \in R, s \in S\}.$$

Addition and multiplication are done in each coordinate. So,

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

and

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

Example: $(a,b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$, then $a \in \mathbb{Z}_2$ and $b \in \mathbb{Z}_3$.
$(1,1) + (1,1) = (0,2)$, since $2 \equiv 0 \mod 2$.
$(0,2) + (1,1) = (1,0)$, since $3 \equiv 0 \mod 3$.
$(1,2) \cdot (0,2) = (0,1)$.
The additive/multipicative identities in $R \oplus S$ are $(0,0)$ and $(1,1)$.
Is $\mathbb{F} \oplus \mathbb{F} =^{defn} \mathbb{F}^2$ a field, or just a ring?

Ring homomorphisms

Let R, S be rings. A **ring homomorphism** is a function $\phi : R \to S$ such that $\phi(1) = 1$ and $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$, for all $r_1, r_2 \in R$.

A ring homomorphism is an **isomorphism** if it is 1-1 and onto.

Example (reduction mod n): Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(m) = [m]$. Addition being preserved ($\phi(a+b) = \phi(a) + \phi(b)$) means $[a+b] = [a] + [b]$. Multiplication is similar. See Proposition 1.4.2 (compare to Proposition 4.3.4 on polynomial congruence).

For this example, what subset of $\mathbb{Z}$ is sent to $[0]$?

Note that for any ring homomorphism ϕ, $\phi(0) = 0$ since for any $r \in R$,

$$\phi(0) + \phi(r) = \phi(0 + r) = \phi(r) = 0 + \phi(r).$$

Other examples:

projection to a coordinate

Define $\phi : R^2 \to R$ by $\phi((r_1, r_2)) = r_1$. Check this is a homomorphism.

Is there any ring homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}$? (Think about the fact that $\phi(1) = 1$, $\phi(1+1) = \phi(1) + \phi(1) = 1 + 1$, etc.)