Last Monday,

<u>Def</u> A field is a *commutative* ring $(F, +, \times)$

- $(F, +)$ is a group with identity element 0 (G2) w.r.t. $+$ for $(F, +)$
- $(F - \{0\}, \times)$ is a group with identity element 1 (G2) w.r.t. $\times$ for $(F - \{0\}, \times)$

- $1 \neq 0$

Rk If $1 = 0$,

then for any $a \in F$

$$a \underset{\uparrow}{=} a \times 1 \overset{\text{assumption.}}{=} a \times 0 \overset{\text{Prop 19.}}{=} 0$$

because 1 is the multiplicative identity

To sum up, if $1 = 0$,

then $F = \{0\}$

Therefore the last field axiom

stops it happening.

Another way of saying this is that $\{0\}$ can NOT be a field.

$0+0=0$

$0\times 0=0$

Example $\mathbb{C}$

$(\mathbb{R},+,\times)$

Def A division ring is a ring that satisfies all the field axioms (include $1\neq 0$) except $ab=ba$ $\forall a,b$

Example Hamilton's quaternions

$$\{ c \cdot 1 + c(p)\,p + c(q)\,q + c(r)\,r \}$$

$$c,\ c(p),\ c(q),\ c(r) \in \mathbb{R}$$

$\underline{1}$, p, q, r are symbols

subject to the relations

$$1 \cdot p = p \cdot 1 = p$$

$$1 \cdot q = q \cdot 1 = q$$

$$1 \cdot r = r \cdot 1 = r$$

$$p^2 = q^2 = r^2 = pqr = -1$$

A division ring is an example of a ring that is not a field.

fields $<$ division rings

$\cap$

rings

$\cap$

Groups

But we've seen more examples

of rings that are not fields

(are not division rings)

Recall $\mathbb{Z}_n$ = the set of equiv classes w.r.t. $\equiv \bmod n$

n: a positive integer n

- $(\mathbb{Z}_n, +)$ is a abelian group with identity $[0]$

- $(\mathbb{Z}_n, +, \times)$ is a commutative ring with identity

[1].

- If n is a prime number p,

then $\mathbb{Z}_p$ is a field.

$$\mathbb{Z}_p = \mathbb{F}_p$$

Rk If n is NOT a prime number,

then $\mathbb{Z}_n$ is NOT a field.

(Think about $\mathbb{Z}_6$!)

§ Polynomials

Def Let $(R, +, \times)$ be a ring.

A polynomial f in one variable X with coefficients in R is

$$f = f(X) = C_n X^n + C_{n-1} X^{n-1} + \cdots + C_1 X + C_0$$

where $C_i \in R$.

The C_i's are called the coeffts of f.

Example $R = \mathbb{Z}$ $\quad x^2 + 17x + 1$

$R = \mathbb{C}$ $\quad x^3 + (1+i)x^2 + i$

Def Let $R[x]$ denote the set of all polynomials in one variable with coeffts in R.

Example $\mathbb{R}[x]$

$R = \mathbb{R}$ the set of real numbers

Def Given $f \in R[x]$.

the degree of f, $\deg(f)$, is

defined to be the largest n

for which the coefficient C_n of X^n

is $\neq 0$

the additive identity of R

$C_{n+1} = C_{n+2} = \cdots = 0$

$$f = \underset{\neq 0}{C_n} X^n + C_{n-1} X^{n-1} + \cdots + C_1 X + C_0$$

Then $\deg(f) = n$.

<u>Example</u> $\deg(X^3 + X^2 + 1) = 3$

Theorem 25 Let $(R, +, \times)$ be a ring.

Then $R[x]$ is a ring w.r.t.

addition: $f+g$

$$(f+g)(x) = f(x) + g(x)$$

$$= \sum_{n=0}^{\max(\deg(f), \deg(g))} (c_n(f) + c_n(g)) \, x^n$$

Ex $(x^5 + x^3 + x + 1)$

$=$

$+ (x^2 + x + 2)$

$$= 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 2x + 3$$

$$C_5(f) + C_5(g) = 1 + 0$$

$$C_4(f) + C_4(g) = 0 + 0$$

$$C_3(f) + C_3(g) = 1 + 0$$

Multiplication $f \times g$ (or fg)

$$(fg)(x) = f(x)\,g(x)$$

$$= \sum_{n=0}^{\deg(f)+\deg(g)} \underline{C_n(fg)}\, x^n$$

where

$$C_n(fg) = \sum_{r=0}^{n} C_r(f)\, C_{n-r}(g)$$

$$= C_0(f)C_n(g) + C_1(f)C_{n-1}(g)$$

$$+ C_2(f)C_{n-2}(g) + \cdots +$$

$$+ \cdots + C_{n-1}(f)C_1(g) + C_n(f)C_0(g)$$

If R is a ring with identity, then so is $R[x]$.

If R is commutative,

then so is $R[x]$.

Proof Possibly on Monday.

Prop 26 If $(R, +, \times)$

is a ring with identity,

then $R[x]$ is NOT a division ring.