G is a group

$H < G$
subgroup

$H * H = H$

$H * H \subseteq H$

Why $H * H = H$?

$1 \in H$

$g_1 H * g_2 H = g_1 g_2 H$

$$g_1 h_1 g_2 h_2 = g_1 g_2 h_3$$

g_1^{-1} $\quad h_1 g_2 h_2 = g_2 h_3$

g_2^{-1} $\quad g_2^{-1} h_1 g_2 h_2 = h_3$

$g_2^{-1} h_1 g_2 = h_3 h_2^{-1}$

$h_1 g_2 h_2 = g_2 h_3$

$h_1 g_2 = g_2 h_3 h_2^{-1}$

$h_1 = g_2 \underbrace{h_3 h_2^{-1}}_{\in H} g_2^{-1}$

$H < G$ is called a <u>normal</u> subgroup iff

$\forall g \in G \quad gHg^{-1} = H$

We write $H \trianglelefteq G$ instead of $H < G$

A group is <u>simple</u> iff it has no non-trivial normal subgroups. $\{1\}$ & G are normal

$g 1 g^{-1} = 1$

If $H \trianglelefteq G$, we can create a new group

$G/H = \{gH \mid g \in G\}$ $\quad g_1 H g_2 H = g_1 g_2 H$

$g_1 H g_2 H = g_1 g_2 H$

$H \trianglelefteq G \quad g_1 H g_1^{-1} = H \implies g_1 H = H g_1$

G/H is a group.

If G is abelian and $H < G \implies H \triangleleft G$

$gHg^{-1} = gg^{-1}H = H$ if G is abelian

$\mathbb{Z}/n\mathbb{Z}$ modulo group.

$\{gH\}$ are the ~~left cosets~~ of H

right cosets

$\{Hg\}$

in general $gH \neq Hg$

When is $gH = Hg$?

$gHg^{-1} = H$

Left cosets = Right cosets if H is normal.

$H < G \implies |H| \mid |G|$

$|G| =$ prime

G is cyclic and any $g \neq 1$ generates

$G \quad |G| = p_1 p_2$

Homomorphisms.

G_1, G_2 are groups

$f : G_1 \longrightarrow G_2$

$f(1_{G_1}) = 1_{G_2}$

$f(a *_1 b) = f(a) *_2 f(b)$

$f(1) = 1$

$f(a*b) = f(a)*f(b)$

$f(g^{-1}) = f(g)^{-1}$

$1 = gg^{-1}$

$1 = f(1) = f(gg^{-1}) = f(g)f(g^{-1})$

$1 = f(g)f(g^{-1})$ so $f(g^{-1}) = f(g)^{-1}$

$g = g*1$ $\quad f(g) = f(g)*f(1)$

$1 = f(1)$

G_1 & G_2 groups

$f: G_1 \to G_2$ hom

$\ker(f) = \{g \mid f(g) = 1\}$

<u>Thm</u> $f: G_1 \to G_2$ is a hom

$\ker(f) < G_1$

<u>Pf:</u> $f(1) = 1$ ~~so~~ $1 \in \ker(f)$

$a, b \in \ker(f)$ $\quad f(a) = 1$ & $f(b) = 1$

$f(ab) = f(a)*f(b) = 1*1$

$a, b \in \ker(f) \Rightarrow ab \in \ker(f)$

so $\ker(f)$ is a subgroup of G_1

<u>Thm</u> $\ker(f) \trianglelefteq G$

$a \in \ker(f)$ $\quad f(a) = 1$

$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)f(g^{-1}) = 1$

$a \in \ker(f)$ $\quad gag^{-1} \in \ker(f)$ $\forall g \in G$

$G/\ker(f)$

<u>Rings</u>

Groups have one operation $*$
Rings have two operations $+, *$
$(R,+,*)$ is a ring iff
$(R,+)$ is an abelian group
and $*$ is associative with identity and the distributive laws

R is a ring iff $(R,+)$ is Abelian group
$0 \in R$ [+ identity] $0+a = a+0 = a$
$1 \in R$ $1*r = r*1 = r$
$*$ is associative
$r*(s+t) = r*s + r*t$
$(s+t)*r = s*r + t*r$

What's missing?

no inverses for $*$
not commutative

$s*0 = 0$

$s*(0+0) = s*0$
$= s*0 + s*0$

$s*0 + s*0 = s*0$
$g+g = g$
$g = 0$

Examples of Rings $(\mathbb{Q},+,*)$ $(\mathbb{R},+,*)$
$(\mathbb{Z},+,*)$

Polynomials $\mathbb{Z}[x]$
$\mathbb{Q}[x]$
$\mathbb{R}[x]$

$$
\begin{array}{r}
x^3+5x^2-7x+3 \\
-x^3-5x^2+7x-3 \\
\hline
\end{array}
$$

$1, 2$

$\mathbb{K}[x]$

$$\frac{f(x)}{g(x)} \text{ with } f(x), g(x) \in \mathbb{Q}[x] \quad g(x) \neq 0$$

x^2

$(\mathbb{C}, +, *)$ $\quad \mathbb{C}[x]$

$$\frac{f(x)}{g(x)} \quad f, g \in \mathbb{C}[x] \quad g \neq 0$$

$n \times n$ matrices $M = [m_{ij}]$ $\quad N = [n_{ij}]$

$M + N =$

$M + N = [m_{ij} + n_{ij}]$

$M * N = [m_{ij} * n_{ij}]$

$M * N = \left[\sum_{k=1}^{n} m_{ik} n_{kj}\right]$

$CF = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous} \}$

$+$

$*$

Ring Homomorphism

$f : R_1 \longrightarrow R_2$

$f(a+b) = f(a) + f(b)$

$f(ab) = f(a)f(b)$

$f(x) = ?$

$= f(a)f(b) + f(a)f(c)$

$f(0) = f(0+0) = f(0) + f(0)$ $\quad$ $f(a(b+c)) = \ldots$

$f(0) = 0$

$f(a) = f(a \cdot 1) = f(a) f(1)$

$f(1) = ?$

Not every definition of ring includes 1.