Rings

Def. A ring is a set R with two binary operations $+$ and $\cdot$ satisfying the following axioms:

1. $+$ is commutative:
   $\forall a, b \in R \quad a+b = b+a$

2. $+$ is associative:
   $\forall a, b, c \in R, \quad (a+b)+c = a+(b+c)$

3. zero:
   $\exists\, 0 \in R$ such that $\forall a \in R, \quad 0+a = a$

4. negatives:
   $\forall a \in R \ \exists\, (-a) \in R$ such that $a+(-a) = 0$

5. $\cdot$ is associative:
   $\forall a, b, c \in R \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

6. one:
   $\exists\, 1 \in R$ such that $\forall a \in R, \quad 1 \cdot a = a \cdot 1 = a$
   and $1 \neq 0$

7. distributive property:
   $\forall a, b, c \in R \quad a \cdot (b+c) = a \cdot b + a \cdot c$
   $(a+b) \cdot c = a \cdot c + b \cdot c$

we don't require $\cdot$ to be commutative
$\forall a, b \in R,\quad a\cdot b = b\cdot a$
if it holds, R is "commutative"

also don't require mult. inverses
$\forall a \in R$ if $a \neq 0$ then $\exists\, (a^{-1}) \in R$
such that $a\cdot(a^{-1}) = (a^{-1})\cdot a = 1$
if this holds, R is a "division algebra"

Examples: 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

2) Some subsets of $\mathbb{R}$ or $\mathbb{C}$:

$$A = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}$$

if I add, subtract, multiply elements of A then I stay inside A.

(notice that $\{ a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z} \}$ is not a ring.
closed under $+$ and $-$ but not $\cdot$)

Rings are places where you can ask about factorization.

7 is prime in $\mathbb{Z}$, but in A we have
$$(3+\sqrt{2})(3-\sqrt{2}) = 9 + 3\sqrt{2} - 3\sqrt{2} - 2 = 7$$

but 3 and 5 are still prime in A...

③ polynomial rings.

$\mathbb{Z}[x]$ = things of the form

$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

where $a_i \in \mathbb{Z}$

know how to $+$ and $\cdot$ these from school.

$\mathbb{R}[x]$ = same, but allow coefficients $a_i \in \mathbb{R}$

$\mathbb{C}[x]$ = - - - - - - - - - - $\mathbb{C}$

factoring: x^4+1 can't be factored in $\mathbb{Z}[x]$

except as $(-1)(-x^4-1)$

in $\mathbb{R}[x]$, $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$

in $\mathbb{C}[x]$, $x^4+1 = \left(x+\frac{1+i}{\sqrt{2}}\right)\left(x+\frac{1-i}{\sqrt{2}}\right)$(two more)

④ ring of functions $\{f : \mathbb{R} \to \mathbb{R}\}$

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

multiply: $(f \cdot g)(x) = f(x) \cdot g(x)$

zero: constant function 0

one: " - - - 1

or just continuous functions

or just differentiable functions...

⑤ matrix rings.

$$M = \left\{ 2\times 2 \text{ matrices } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a,b,c,d \in \mathbb{Z} \right\}$$

or $\in \mathbb{R}$

or $\in \mathbb{C}$

add: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & w \end{pmatrix}$

$$= \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix}$$

multiply: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}$

what is 0 in this ring M?

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

what is 1?

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

M is not commutative:

if $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ then $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.