In this course we will study *fields*, *rings*, *polynomial rings* and *groups*
(See page 191-192 of Section 4.1, pages 236-238 of Section 5.1, and page 95 of Section 3.1).

Here is the formal definition of a *field,* which I give first because you have used fields in all your previous mathematics and science courses.

**4.4.1 Definition**. Let $F$ be a set on which two binary operations are defined, called **addition** and **multiplication**, denoted by $+$ and $\cdot$ respectively. That is the following conditions must be satisfied

**(i)** ***Closure*****:** For all $a, b \in F$ the sum $a + b$ and the product $a \cdot b$ are well-defined elements of $F$.

Then $F$ is called a ***field*** with respect to the operations if the following properties hold.

**(ii)** ***Associative Laws*****:** For all $a, b, c \in F$,

$$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c \ .$$

**(iii)** ***Commutative Laws***: For all $a, b \in F$,

$$a + b = b + a \text{ and } a \cdot b = b \cdot a \ .$$

**(iv)** ***Distributive Laws*****:** For all $a, b, c \in F$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and } (a + b) \cdot c = (a \cdot c) + (b \cdot c) \ .$$

**(v)** ***Identity Elements*****:** The set $F$ contains an element 0, called the ***additive identity element***, such that for all $a \in F$,

$$a + 0 = a \text{ and } 0 + a = a \ .$$

The set $F$ also contains an element 1 (required to be different form 0), called the ***multiplicative identity element***, such that

$$a \cdot 1 = a \text{ and } 1 \cdot a = a \ .$$

**(vi)** ***Inverse Elements*****:** For each $a \in F$, the equations

$$a + x = 0 \text{ and } x + a = 0$$

have a solution $x \in F$, called an ***additive inverse*** of $a$, and denoted by $-a$.
Also, for each ***nonzero*** element $a \in F$, the equations

$$a \cdot x = 1 \text{ and } x \cdot a = 1$$

have a solution $a \in F$, called a ***multiplicative inverse*** of $a$, and denoted by $a^{-1}$.

■

**Examples**: The *rational numbers*, the *real numbers* and the *complex numbers* denoted by $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ respectively are all examples of fields with an infinite number of elements. Examples of finite fields will be presented later.

Next, we define a *ring* in terms of a *field*. A formal definition is given on pages 236-238 of the text.

**Definition**: Let $A$ be a set on which two binary operations are defined, called **addition** and **multiplication**, denoted by $+$ and $\cdot$ respectively. Then $A$ is called a ***commutative ring*** if all the properties of a field are satisfied ***except*** for the multiplicative inverse property. If the commutative property for ***multiplication*** is ***not*** satisfied, then A is called a **noncommutative ring**. ∎

**Examples**:

1. The integers $\mathbf{Z}$ is a commutative ring.

2. $\mathbf{Z}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\,\middle|\, a,b\in\mathbf{Z}\right\}$ is a *commutative* ring since it is closed under addition and multiplication. More generally, if $c\in\mathbf{Z}$ isn't a perfect square (that is, not the square of an integer), then $\mathbf{Z}\left[\sqrt{c}\right]=\left\{a+b\sqrt{c}\,\middle|\, a,b\in\mathbf{Z}\right\}$ is a commutative ring since it is closed under addition and multiplication. Rings of this form are studied in number theory.

3. The set of all two by two matrices with real numbers as entries $M_2[\mathbf{R}]=\left\{\begin{pmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{pmatrix}\middle| r_{1,1},r_{1,2},r_{2,1},r_{2,2}\in\mathbf{R}\right\}$ is a *noncommutative* ring where addition and multiplication defined in the usual manner for matrices. In this case, the ***additive identity*** is $\mathbf{0}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and ***multiplicative identity*** is $\mathbf{I}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. More generally, if $A$ is a *commutative* ring, then $M_2[A]=\left\{\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}\middle| a_{1,1},a_{1,2},a_{2,1},a_{2,2}\in A\right\}$ with addition and multiplication defined in the usual manner for matrices is a *noncommutative* ring.

**4.1.4 Definition**: Let $F$ be a field. If $a_n,a_{n-1},\ldots,a_1,a_0\in F$ (where $n$ is a nonnegative integer), then any expression of the form

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

is called a ***polynomial over*** $F$ in the ***indeterminate*** $x$ with ***coefficients*** $a_m,a_{m-1},\ldots,a_1,a_0$. The subscript $i$ of the coefficient $a_i$ is called its ***index***.

If $n$ is the largest nonnegative integer such that $a_n\neq 0$, then we say that the polynomial $f(x)=a_nx^n+\cdots+a_0$ has ***degree*** $n$, written $\deg(f(x))=n$ and $a_n$ is called the ***leading coefficient*** of $f(x)$. If $a_0$ is the leading coefficient of $f(x)$, then $f(x)$ is called a ***constant polynomial***. Also, if the leading coefficient of $f(x)$ is 1, then $f(x)$ is called a ***monic polynomial***. The set of all polynomials with coefficients in $F$ is denoted by $F[x]$. It is also referred too as the ***ring of polynomials over*** $F$; that is, $F[x]$ is a commutative ring! ∎

**Examples**: The rings of polynomials over $\mathbf{Q},\mathbf{R},\mathbf{C}$ are denoted by $\mathbf{Q}[x],\mathbf{R}[x],\mathbf{C}[x]$ respectively.
Note that $\mathbf{Q}[x]\subset\mathbf{R}[x]\subset\mathbf{C}[x]$ since $\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$.

Finally, here is the definition of a group. I've left it to last because

1. *You have all have used fields, rings, polynomial rings and matrix rings in your previous courses even if you did not know their formal names and definitions!*
2. *Many people find the definition of a group to be more abstract than the other definitions!*

**3.1.4 Definition**. Let $(G,*)$ denote a *nonempty* set $G$ together with a binary operation $*$ on $G$ that satisfies the following condition:

**(i) *Closure***: For all $a,b \in G$, the element $a*b$ is a well-defined element of $G$.

Note: If only the *closure* condition (or property) is satisfied $(G,*)$ is called a set with a binary operation.

For $(G,*)$ to be a ***group*** the following additional conditions must also be satisfied.

**(ii) *Associativity*:** For all $a,b,c \in G$, we have $a*(b*c)=(a*b)*c$.

**(iii) *Identity***: There exists an identity element $e \in G$, that is, an element $e \in G$ such that $e*a=a$ and $a*e=a$ for all $a \in G$.

**(iv) *Inverses***: For each $a \in G$ there exists an inverse element $a^{-1} \in G$, that is an element $a^{-1} \in G$ such that $a*a^{-1}=e$ and $a^{-1}*a=e$.

If, in addition, the commutative property holds for $(G,*)$, that is, $a*b=b*a$ for all $a,b \in G$, then $(G,*)$ is called a **commutative group**. In this case, $+$ is often used to denote the binary operation instead of * and $0$ is used to denote the identity element instead of *e.* The element $-a$ is often used to denote an inverse element for $a \in G$. Moreover, the binary operation is often called *addition*. ∎

Note: When only one binary option * is involved or is well-known, the notation $(G,*)$ is often simplified to $G$.

**Examples**: 1. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ and $\mathbf{C}$ under the usual addition operations all form commutative groups.

2. $\mathbf{Z}\left[\sqrt{c}\right]=\left\{a+b\sqrt{c}\,\middle|\, a,b \in \mathbf{Z}\right\}$ under the usual *addition* operation forms a *commutative* group.

3. $M_2[\mathbf{R}]=\left\{\begin{pmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{pmatrix}\middle| r_{1,1}, r_{1,2}, r_{2,1}, r_{2,2} \in \mathbf{R}\right\}$ under the usual matrix *addition* is a *commutative* group.

4. Any vector space under its operation of addition is a *commutative* group!

5. Let $\mathbf{R}^{\times}=\left\{r \in \mathbf{R}\middle| r \neq 0\right\}$. Then $\mathbf{R}^{\times}$ under the usual multiplication of real numbers forms a group called the multiplicative group of the nonzero real numbers. More generally, if $F$ is any field, let $F^{\times}=\left\{a \in F\middle| a \neq 0\right\}$.

Then $F^{\times}$ under the multiplication of $F$ forms a group called the *multiplicative group of the nonzero elements* of the field *F.*

6. Let $\mathbf{GL}_2[\mathbf{R}]=\left\{m \in \mathbf{M}_2[\mathbf{R}]\middle|\det(m) \neq 0\right\}$ under the usual matrix multiplication operation forms a *noncommutative* group. Note that if $m=\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$, then $m^{-1}=\dfrac{1}{\det(m)}\begin{pmatrix} a_{2,2} & -a_{2,1} \\ -a_{1,2} & a_{1,1} \end{pmatrix}$ where $\det(m)=a_{1,1}a_{2,2}-a_{1,2}a_{2,1} \neq 0$.