LECTURE 6  Rings and Fields

Inspired by the fact that we have seen some laws hold for both integers, complex numbers, matrices, polynomials etc, we make the following definition:

Def A set $R$ together with two binary operations $+, \cdot : R \times R \to R$ is called a ring if the following holds:

(A1) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$  
(associativity of addition)

(A2) $a + b = b + a$ for all $a, b \in R$  
(commutativity of addition)

(A3) There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$  
(existence of zero)

(A4) For every $a \in R$, there is an element $-a \in R$ such that $a + (-a) = 0$  
(existence of additive inverse)

(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$  
(associativity of multiplication)

(D) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$  
(distributivity)
Ex \((\mathbb{Z}, +, \cdot)\) with \(+\) and \(\cdot\) as ordinary addition and multiplication. Also \(\mathbb{R}, \mathbb{Q}, \mathbb{C}\) with ordinary multiplication and addition.

Ex \(2\mathbb{Z}\) - the set of all even integers. Subset of \(\mathbb{Z}\). First check that \(a, b \in 2\mathbb{Z}\) \(\implies a + b\) and \(a \cdot b \in 2\mathbb{Z}\). Yes, true.
Then \(A_1, A_2, M_1\) and \(D\) are inherited from \(\mathbb{Z}\). What we need to check is that \(0 \in 2\mathbb{Z}\) (Yes it does) and that inverses of even numbers are also even (Yes, also true).

This shows that \(2\mathbb{Z}\) is a ring.

Ex The set of odd numbers is not a ring since the sum of two odd numbers is even.

In the above examples of rings we also have that \((M_2)\) \(a \cdot b = b \cdot a\) for all \(a, b \in R\) holds (commutativity of multiplication).

Such rings are called commutative rings.
The set \( M_2(\mathbb{R}) \) of all 2x2 matrices with real entries is a ring. The zero is \((0,0)\) and the (additive) inverse of \((a, b, c, d)\) is \((-a-b, -c-d)\). The laws A1, A2, M1, D are known from linear algebra.

It's easy to show that this is a non-commutative ring. For example with \(A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \) \(B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\) we have \(AB = \begin{pmatrix} 4 & 6 \\ 4 & 6 \end{pmatrix}\) and \(BA = \begin{pmatrix} 3 & 3 \\ 7 & 7 \end{pmatrix}\) so \(AB \neq BA\).

Moreover \( M_2(\mathbb{R}) \) has zero-divisors:
\[
\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\]

**Def.** Two elements \(a \neq 0, b \neq 0\) are called zero-divisors if \(a \cdot b = 0\).

**Rings with unity.**
Most rings we will encounter have property (M3) there is an element \(1 \in R\) such that \(1 \cdot a = a \cdot 1 = a\) for all \(a \in R\).

**Ex.** In \(\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}\) the number 1 is the unity.
In \(\mathbb{Z}\) there is no unity because \(2k(2k) = 2(2k^2) = 4k^2 \neq 2k\) for all \(k \in \mathbb{Z}\) has no solution.
In $M_2(\mathbb{R})$ the unity is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

**Def:** A commutative ring with unity such that

$$(H4)$$ for every $a \neq 0$ in $A$ there is $a^{-1} \in A$ such that $a \cdot a^{-1} = 1$ holds is called a field

**Ex:** Considering our examples of commutative rings with unity we find that

$\mathbb{R}, \mathbb{C}, \mathbb{C}$ are fields using $\frac{1}{a}$ as $a^{-1}$

In $\mathbb{Z}$ however $\frac{1}{a}$ is usually not in the ring

E.g. $\frac{1}{2}$ is not an integer. In fact the only invertible elements in $\mathbb{Z}$ are $\pm 1$. For other $a \in \mathbb{Z}$ we cannot find any $b \in \mathbb{Z}$ with $a \cdot b = 1$, $\mathbb{Z}$ is not a field.

$\mathbb{Z}$ has no unity and $M_2(\mathbb{R})$ is not commutative so they do not qualify as fields.

**Rings of congruency classes**

Let $n$ be an integer $\geq 2$. We say that two integers $a, b$ are congruent modulo $n$ (written $a \equiv b \pmod{n}$) if $n$ divides $a - b$. 
Congruence modulo $n$ is an equivalence relation (reflexive: $a \equiv a$, symmetric $a \equiv b \Rightarrow b \equiv a$, and transitive $a \equiv b$ and $b \equiv c \Rightarrow a \equiv c$)

Therefore it partitions the integers into disjoint equivalence classes. Denote the class containing $a$ by $[a]$. 

We want to make the set of classes $R = \{[0], [1], [2], \ldots, [n-1]\}$ into a ring by defining $+$ and $\cdot$.

Let $[a] + [b] = [a+b]$ and $[a] \cdot [b] = [a \cdot b]$.

We need to check that our $+$ and $\cdot$ are well defined, that is that the result is independent of choice of representatives $a, b$ of the classes involved. If $a', b'$ are other representatives of those classes then $a-a' = k \cdot n$ and $b-b' = l \cdot n$ for some integers $k, l$.

Hence $[a'] + [b'] = [a'+b'] = [a-k \cdot n + b-l \cdot n] = [a+b]$. 

\[ \uparrow \text{by def} \]
\[ [a+b+n(-k-l)] = [a+b] \]
so + is well defined.  
For + we have:
\[ [a'] + [b'] = [a' + b'] = [(a - kn)(b - ln)] = [ab + n(kln - kb - la)] = [ab] \] showing that this operation is also well defined.

The axioms (A1)-(A4), (M1) and (D) are now easy to show because they hold for the integers.

The ring of classes modulo \( n \) is called \( \mathbb{Z}/n \)
It is commutative and has unity [1]


This shows that there are zero divisors in \( \mathbb{Z}_6 \)
A zero divisor is not invertible (show as an exercise!) so \( \mathbb{Z}_6 \) cannot be a field.

\[ \text{Ex } \] in \( \mathbb{Z}_7 \) \( [1][1] = [1] \)
\( [2][4] = [8] = [1] \)
\( [3][5] = [15] = [1] \)
\( [6][6] = [36] = [1] \)

So all elements \( \neq [0] \) are invertible
\( \mathbb{Z}_7 \) is a field
In general \( Z_n \) is a field if \( n \) is prime but otherwise not as we will see later on.

**Thm 1.7** \([a] = [0] \iff Z_n \) has an inverse \( \iff (a,n) = 1 \)

**Proof:** Assume first that \((a,n) = d \geq 2\). Then \(a = d a', n = d n'\) and \([a][n'] = [a \cdot n'] = [d a' n'] = [dn] = [0]\).

\([a]\) is zero divisor \(\iff [a] \) has no inverse

Assume now instead that \((a,n) = 1\). Then using the Euclidean algorithm on \(a\) and \(n\) and back substituting we find \(b, c \in \mathbb{Z}\) such that \(1 = a \cdot b + n \cdot c\). In \(Z_n\) this becomes \([1] = [a] [b]\) so \([b]\) is an inverse of \([a]\)

**Ex** Find the inverses of \([42]\) and \([70]\) in \(Z_{275}\) if they exist.

First check if 42 and 70 have common prime factors with 275:

\[42 = 2 \cdot 3 \cdot 7, \quad 70 = 2 \cdot 5 \cdot 7, \quad 275 = 5^2 \cdot 11\]

\(\iff (42,275) = 1\) \([42]\) has an inverse \(\iff (70,275) = 5\) \([70]\) has no inverse
Compute \([42]^{-1}\)

Euclidean algorithm:

\[
275 = 6 \cdot 42 + 23 \\
42 = 2 \cdot 23 + 4 \\
23 = 4 \cdot 6 - 1
\]

\[1 = 4 \cdot 6 - 23 = \]
\[= (42+2 \cdot 23) \cdot 6 - 23 = \]
\[= 4 \cdot 23 + 6 \cdot 42 = \]
\[= 11 (275 - 6 \cdot 42) - 6 \cdot 42 = \]
\[= 11 \cdot 275 - 72 \cdot 42
\]

Hence \(1 = 11 \cdot 275 - 72 \cdot 42 \Rightarrow \left[1\right] = \left[-72\right] \cdot \left[42\right]\)

so \([42]^{-1} = \left[-72\right] = \left[203\right]\)

Ans: \([70]\) has no inverse in \(\mathbb{Z}_{275}\) and
\([42]^{-1} = \left[203\right]\)

Thus \(\mathbb{Z}_n\) is a field \(\Leftrightarrow n\) is a prime

Proof: Follows immediately from the previous theorem since \((a, p) = 1\) for all \(a\) between \(1\) and \(p-1 \Leftrightarrow p\) is prime.