Notes for 7 Feb (Thursday)

1 The road so far...

1. Did modular arithmetic and defined an equivalence relation.
2. Main point - "You are invertible if you are coprime".

2 Rings and Fields

It is high time we defined rings. Let us recall the definition of a group : A group $(G, *)$ is a set G with a binary operation $* : G \times G \to G$ satisfying

1. Associativity : $(a * b) * c = a * (b * c)$.
2. Existence of identity : $\exists e$ such that $a * e = e * a = a$ for all $a \in G$.
3. Existence of inverses : For every $a \in G$, there exists a b_a such that $b_a * a = a * b_a = e$.

We proved that inverses and identity are unique in a group. If commutativity holds, such a group is called an Abelian group. An example of an Abelian group is $\mathbb{Z}$ and that of a non-Abelian group is S_n. (Also, invertible 2×2 matrices of real numbers.)
A ring $(R, +, ., 0, 1)$ is a set R with two binary operations $+, . : R \times R \to R$ and two distinguished elements 0 (the additive identity) and 1 (the multiplicative identity) satisfying

1. $(R, +, 0)$ is an Abelian group. So 0 is unique.
2. $(R, ., 1)$ is a monoid, i.e., associativity and existence of identity hold (but not necessarily inverses). So 1 is unique.
3. Distributivity holds : $a.(b + c) = a.b + a.c, (b + c).a = b.a + c.a$.

If multiplication is commutative, such a ring is called a commutative ring. (A very important class of rings.) Here are examples and non-examples of rings :

1. $(\mathbb{Z}, +, \times, 0, 1)$ is a commutative ring.
2. $(\mathbb{Q}, +, \times, 0, 1)$ is a commutative ring.
3. $(Mat(n, \mathbb{R}), +, \times, [0]_{n\times n}, Id_{n\times n})$ is a non-commutative ring.

4. Polynomials in any fixed number of variables with integral coefficients form a commutative ring.

5. Continuous functions from $\mathbb{R}$ to $\mathbb{R}$ form a commutative ring.

6. $(\{Even, Odd\}, +, ., even, odd)$ is a commutative ring. This ring is finite in cardinality (unlike all the above ones).

7. $\mathbb{R}^3$ under vector addition and cross product do not form a ring because associativity is lost.

8. $(\{Positive, 0, Negative\}$ cannot be made into a ring in the usual way because addition is ill-defined.

9. $\mathbb{N}$ is not a ring in the usual way because addition is not a group.

10. $\mathbb{R}_+$ is not a ring for the same reason.

The point of rings is that you can pretend they are like integers. A subring S of $(R, +, ., 0, 1)$ is a subset of R containing $0, 1$ such that $(S, +, ., 0, 1)$ is a ring. For S to be a subring, it simply needs to be closed under addition, multiplication, and additive inverses. For instance, $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are subrings of $\mathbb{C}$.

An element a of a commutative ring is called a unit if it has a multiplicative inverse. For example, non-invertible matrices are not units. By the way, the set of units is a group under multiplication. Indeed, if a, b have inverses, then $(a.b)^{-1} = a^{-1}b^{-1}$.

A field $(F, +, ., 0, 1)$ is a commutative ring with at least 2 elements (i.e., $0 \neq 1$) where every non-zero element has a multiplicative inverse, i.e., $(F - \{0\}, ., 1)$ is an Abelian group, or alternatively, all the non-zero elements are units. Here are examples and non-examples of fields :

1. $(\mathbb{Z}, +, \times, 0, 1)$, $(Mat(n, \mathbb{R}), +, \times, [0]_{n\times n}, Id_{n\times n})$ are not fields because of lack of multiplicative inverses.

2. $(\mathbb{Q}, +, \times, 0, 1)$, $(\mathbb{R}, +, \times, 0, 1)$, and $(\mathbb{C}, +, \times, 0, 1)$ are fields.

3. $(\{Even, Odd\}, +, ., even, odd)$ is a field. This field is a finite field.

4. Polynomials with integral (or even real) coefficients do not form a field.

5. Rational functions with rational (or real or complex) coefficients form a field.

The point of fields is that you can pretend that they are basically like rational numbers.

An important example of a ring is furnished by the quotient set of $\mathbb{Z}$ under the equivalence relation $\equiv_m$. Recall that $a \equiv_m b$ iff $a = b + km$. The quotient set (i.e. set of equivalence classes) is written as $\mathbb{Z}/m\mathbb{Z}$. Every element is written as $[a]_m$ (the integer a is said to be a representative of the equivalence class). We can define

1. Addition : $[a]_m + [b]_m := [a+b]_m$. Addition is well-defined because $a' + b' \equiv_m a + b$. Addition is a group with $[0]_m$ as the additive identity.

2. Multiplication : $[a]_m[b]_m := [ab]_m$. Likewise, multiplication is well-defined. Multiplication is a monoid with $[1]_m$ as the identity.

Note that $([a]_m + [b]_m)[c]_m = [a+b]_m[c]_m = [ac+bc]_m = [a]_m[c]_m + [b]_m[c]_m$. Therefore, $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring. Note that elements of $\mathbb{Z}/m\mathbb{Z}$ are $\{[0]_m, [1]_m \dots [m-1]_m$. (Another set of representatives is $\{[1]_m, [2]_m, \dots [m]_m$ for instance.) Certainly, $\mathbb{Z}/6\mathbb{Z}$ is not a field because $[2]_6$ has no multiplicative inverse.