we start with recalling definition of ideal and factor ring:

**Def.** Suppose $A$ is a unital (commutative) ring. $I \subseteq A$ is called an ideal of $A$ if $\forall a, b \in I$, $a + b \in I$ and $\forall r \in A$, $a r, r a \in I$.

We write $I \triangleleft A$. (When $A$ is not commutative, left and right ideals are defined as well where the 2nd condition is replaced with $\forall r \in A$, $a r \Rightarrow r a \in I$ and $\forall r \in A$, $r a \Rightarrow a r \in I$, respectively).

* Suppose $I \triangleleft A$. Then on the additive group $A/\mathbb{I}$ one can define the following binary operation: $(a + \mathbb{I})(a_2 + \mathbb{I}) = a_1 a_2 + \mathbb{I}$.

Here is why it is well-defined: $a_i + \mathbb{I} = a_i' + \mathbb{I} \Rightarrow a_i - a_i' \in \mathbb{I}$

$\Rightarrow a_1 a_2 - a_1' a_2' = a_1 a_2 - a_1' a_2 + a_1' a_2 - a_1' a_2' = (a_1 - a_1') a_2 + a_1' (a_2 - a_2') \in \mathbb{I} \Rightarrow a_i a_2 + \mathbb{I} = a_i' a_2 + \mathbb{I}$.

One can check that $(A/\mathbb{I}, +, \cdot)$ is a unital (comm.) ring.

* Suppose $f : A \to A'$ is a ring homo.; that means $f$ is a gp
Lecture 16: Ideals, factor rings, and isomorphism th'm

Wednesday, December 5, 2018  2:53 PM

homo. and it preserves multiplication. Then the following

is a commuting diagram

\[
\begin{array}{ccc}
A & \xrightarrow{f} & \text{Im } f \\ \pi \downarrow & & \downarrow \\
A/\ker f & \xrightarrow{\tilde{f}} & \text{Im } \tilde{f}
\end{array}
\]

(The 1st isomo. theorem)

Going back to ring of poly.; an extremely useful way of studying it is by viewing them as functions:

Evaluation map. Suppose \( A \subseteq B \) is a ring extension.

For \( b \in B \), let \( \phi_b : A[x] \to B \), \( \phi_b(f(x)) = f(b) \). Then \( \phi_b \) is a ring homomorphism. Image of \( \phi_b \) is

\[ \left\{ \sum_{i=0}^{n} a_i b^i \mid a_i \in A, n \in \mathbb{Z}^+ \right\} \]

which is the smallest subring of \( B \) that has \( A \) as a subset and contains \( b \). We denote such ring by \( A[b] \). Warning. This notation is similar to poly. ring, and one has to distinguish them from the content. \( \ker \phi_b = \left\{ \sum_{i=0}^{n} f(x) e_{A[x]} \mid f(b) = 0 \right\} \). \( b \) is a zero of \( f \).

By the 1st isom. \( A[b] \cong A[x]/\left\{ f(x) e_{A[x]} \mid f(b) = 0 \right\} \).
Ex. Show that $\mathbb{Q}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Q}[i] = \{ a + bi | a, b \in \mathbb{Q} \}$.

**Proof.** Consider the evaluation map at $i$. Then

$$\operatorname{Im} \phi_i = \left\{ \begin{array}{ccc}
\sum_{j=0}^{n} r_j (i)^j & | & r_j \in \mathbb{Q}, n \in \mathbb{Z}^+ \\
i^2 & = & 1 \\
i^3 & = & i \\
i^4 & = & -1
\end{array} \right\} \mathbb{Q} = \mathbb{Q}[i].$$

$$\ker \phi_i = \left\{ f(x) \in \mathbb{Q}[x] | f(i) = 0 \right\}$$

For instance $x^2 + 1 \in \ker \phi_i$. If $f(x) \in \ker \phi_i$, then by long division $f(x) = (x^2 + 1) q(x) + r(x)$,

$$q(x), r(x) \in \mathbb{Q}[x], \ deg r < \deg (x^2 + 1) = 2.$$ 

Hence $\exists a, b \in \mathbb{Q}$ s.t. $r(x) = ax + b$.

We plug in $i$ at both sides:

$$0 = f(i) = (i^2 + 1) q(i) + r(i) = ai + b$$

So $a = b = 0$; therefore $r(x) = 0$ and $f(x) \in \langle x^2 + 1 \rangle$.

**Remark.** For a non-empty subset $X$ of a ring $A$, $<X>$ denotes the smallest ideal of $A$ that contains $X$ as a subset.
Lecture 16: Finitely generated ideals

Notice that this is a similar notation as the subgroup generated by $X$, and one has to understand which one is which from the content.

(Since intersection of a family of ideals is an ideal,

\[ <X> = \bigcap_{X \subseteq I \subseteq A} I \]

is the smallest ideal of $A$ that contains $X$ as a subset.)

**Lemma.** For a unital commutative ring $A$, $a_1, \ldots, a_n \in A$,

\[ <a_1, \ldots, a_n> = \{ r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in A \} \]

In particular, a principal ideal $<a> = \{ ra \mid r \in A \}$.

**Pf.** Suppose $a_1, \ldots, a_n \in I$ and $I \subseteq A$. Then

\[ \forall r_1, \ldots, r_n \in A, \ r_1 a_1, \ldots, r_n a_n \in I \Rightarrow r_1 a_1 + \cdots + r_n a_n \in I. \]

\[ \Rightarrow \text{RHS} \subseteq I \Rightarrow \text{RHS} \subseteq \bigcap_{I \subseteq A} I = <a_1, \ldots, a_n>. \]

One can easily check that the RHS is an ideal of $A$; and

\[ a_i = 0 \cdot a_1 + \cdots + 0 \cdot a_{i-1} + i \cdot a_i + 0 \cdot a_{i+1} + \cdots + 0 \cdot a_n \in \text{RHS} \]

\[ \Rightarrow <a_1, \ldots, a_n> \subseteq \text{RHS}. \ And \ we \ get \ (\ast). \)
Def. For \( f(x) \in \mathbb{A}[x] \), we let \( \deg f = -\infty \) if \( f = 0 \), and
\[
\deg f = n \text{ if } f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \text{ and } a_n \neq 0.
\]

Ex. In \( \mathbb{Z}/6\mathbb{Z} [x] \), \( \deg 3x^2 = 2 \), \( \deg 4x + 1 = 1 \),
\[
\deg ((3x^2)(4x + 1)) = \deg 3x^2 = 2 \neq \deg (3x^2) + \deg (4x + 1).
\]

The main reason for \( \deg f_1 f_2 \neq \deg f_1 + \deg f_2 \) is the existence of zero-divisors.

Def. Suppose \( \mathbb{A} \) is a unital commutative ring.

1. \( a \in \mathbb{A} \setminus \{0\} \) is called a zero-divisor if \( \exists b \in \mathbb{A} \setminus \{0\} \) s.t. \( ab = 0 \).
2. For \( a, b \in \mathbb{A} \), we say \( a \mid b \) if \( \exists c \in \mathbb{A} \) s.t. \( b = ac \).
   
   (this is equivalent to say \( \langle b \rangle \subseteq \langle a \rangle \).)
3. \( a \in \mathbb{A} \) is called a unit if \( a \mid 1 \); this means
   \( \exists b \in \mathbb{A} \), \( ab = ba = 1 \).

Def. A non-trivial unital commutative ring \( \mathbb{D} \) is called an integral domain if it has no zero-divisors. (Here non-trivial
Def. A non-trivial unital commutative ring $F$ is called a field if any non-zero element of $F$ is a unit in $F$.

Lemma. (1) The set of units of a ring $R$ is denoted by $R^\times$; and $(R^\times, \cdot)$ is a group.

2) The set of zero-divisors of a unital commutative ring $A$ is denoted by $D(A)$; and $D(A) \cap A^\times = \emptyset$. In particular any field is an integral domain.

Pf. (1) $a, b \in R^\times \implies \exists a', b' \in R$ s.t. $aa' = bb' = 1$; and so $a'a - b'b = 1$, 

$(ab)(b'a') = (b'a')(ab) = 1$, which implies $ab \in R^\times$.

$a \in R^\times \implies \exists a' \in R$ s.t. $aa' = 1 = a'a \Rightarrow a' \in R^\times$ and it is multiplicative inverse of $a$. $11 = 1 \implies 1 \in R^\times$.

(2) Suppose $a \in D(A) \cap A^\times$. Then $\exists b \in A \setminus \{0\}$ s.t. $ab = 0$ and $\exists a' \in A$ s.t. $a'a = 1$. So $b = (a'a)b = a'(ab) = 0$ which is a contradiction. To show the 2nd part of claim.
we first notice that, since $F$ is a field, it is a non-trivial ring. Then we observe that $D(F) \subseteq F \setminus (F^* \cup \{0\})$ as $D(F) \cap F^* = \emptyset$ and $0 \notin D(F)$, which implies $D(F) = \emptyset$.

We notice that $\mathbb{Z}$ is an integral domain, but it is not a field. So an integral domain is not necessarily a field.

Nevertheless under additional conditions we might get such an implication:

**Proposition.** A finite integral domain is a field.

**Proof.** Let $a \in D \setminus \{0\}$, let $f_a : D \to D$, $f_a(b) = ab$.

**Claim.** $f_a$ is 1-1.

**Proof of claim.**

If $f_a(b_1) = f_a(b_2)$, then $a b_1 = a b_2 \Rightarrow a(b_1 - b_2) = 0 \Rightarrow a \neq 0 \Rightarrow b_1 = b_2$.

Since $D$ is finite and $f_a$ is 1-1, $f_a$ is onto. So $\exists b \in D$ st. $f_a(b) = 1$; hence $\exists b \in D$, $ab = 1$, which means $a \in D^*$.

We also mention that $D$ is non-trivial as it is an int. dom.
Remark. When \( D \) is a finite dimensional \( k \)-vector space for some field \( k \) and multiplication in \( D \) is \( k \)-linear (we call such a ring a \( k \)-algebra), the above argument still works:

- \( D: \) integral domain \( \iff D \) is a field.
- \( D: \) finite dimensional \( k \)-algebra

**Lemma.** Suppose \( D \) is an integral domain. Then, for any \( f, g \) in \( D[\mathbb{X}] \), \( \deg fg = \deg f + \deg g \).

(Here we are using the convention that \(-\infty + n = -\infty \) for any \( n \in \mathbb{Z} \) and \((-\infty ) + (-\infty ) = -\infty \).)

**Pf.** If either \( f=0 \) or \( g=0 \), then \( fg=0 \); and so \( \text{LHS} = -\infty \) and \( \text{RHS} = -\infty \).

- Suppose \( f \neq 0 \) and \( g \neq 0 \). So \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) and \( a_n \neq 0 \) and \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0 \) and \( b_m \neq 0 \).

(\( a_n \) is called the leading coefficient of \( f \)). Then

\[
fg(x) = a_n b_m x^{n+m} + \text{terms of deg.} < m+n)
\]
\[ a_n \neq 0, b_m \neq 0 \implies a_n b_m \neq 0. \] And so \( \deg fg = n + m \) no zero-divisor

\[ \deg f + \deg g = \deg f + \deg g. \]

**Cor.** If \( D \) is an integral domain, then \( D[x] \) is an integral domain.

**Prf.** \( f \cdot g = 0 \implies \deg fg = -\infty \implies \deg f + \deg g = -\infty \)

\[ \implies \deg f = -\infty \text{ or } \deg g = -\infty \]

\[ \implies f = 0 \text{ or } g = 0. \]

**Cor.** If \( D \) is an integral domain, then \( D[x] \cong D^x \).

**Prf.** \( f \cdot g = 1 \implies \deg fg = 0 \implies \deg f + \deg g = 0 \)

\[ \implies \deg f, \deg g \in \mathbb{Z}^\circ \implies \deg f = \deg g = 0 \]

\[ \implies \deg f + \deg g = 0 \]

\[ \implies f, g \in D \implies f \in D^x. \]

As it was pointed out earlier, parts of algebra has been developed to solve Fermat’s last conjecture. Roughly idea was; write

\[ x^p - y^p = (x-y)(x-\zeta y)\cdots(x-\zeta^{p-1}y) \quad \text{where} \quad \zeta = e^{\frac{2\pi i}{p}}, \]
if in \( \mathbb{Z}[\zeta] \) we had prime elements and could write any element as a prod. of primes and made sure that \( x-\zeta y \) to be relatively prime, then \( x-y = z_p, x-\zeta y = z_1, \ldots, x-\zeta y = z_p \) for some \( z_i \in \mathbb{Z}[\zeta] \). And we had a chance of getting a contradiction. This is what Kummer did. He further realized that, though in general we do not get the desired unique factor, if we change to ideals we do get such a result; that is why he called ideals, ideal numbers. Later they were studied extensively for other rings, and the word "number" got dropped.

**Def.** Suppose \( A \) is a unital commutative.

1. \( \mathfrak{p} \subseteq A \) is called a prime ideal if
   - \( \mathfrak{p} \) is proper and \( ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \) or \( b \in \mathfrak{p} \).

   The set of all prime ideals of \( A \) is denoted by \( \text{Spec}(A) \).

2. \( \mathfrak{m} \subseteq A \) is called a maximal ideal if
   - \( \mathfrak{m} \) is proper and (\( \mathfrak{m} \subseteq J \subseteq A, J\trianglelefteq A \Rightarrow J=A \))

   The set of all maximal ideals of \( A \) is denoted by \( \text{Max}(A) \).