Note Title 1/5/2012

MATH 3030 ALGEBRA I

Lecture 7

Factorization in commutative rings

As before, R is always a commutative ring with unity $1 \neq 0$.

Def: Let $a, b \in R$. We say a divides b (denoted by $a \mid b$) if $\exists\, c \in R$ s.t. $b = ac$. In this case, a is called a divisor (or factor) of b and b is called a multiple of a.
We write $a \nmid b$ when a does not divide b.
If $a = bc$ and neither b nor c is a unit of R, then we say b (and c) is a proper factor of a

Def: Two elements $a, b \in R$ are called associates in R (denoted by $a \sim b$) if $a | b$ and $b | a$.

Rmks: 1) This defines an equivalence relation on R.

2) If R is an integral domain, then $a \sim b$ iff $\exists u \in R^\times$ (units) s.t. $a = bu$.

Here come two important concepts:

Def: Let $0 \neq a \in R$ which is not a unit. We say that

1. a is irreducible if it has no proper factors.
2. a is prime if $\forall b, c \in R$, $a | bc \Rightarrow a | b$ or $a | c$.

Examples
- In $\mathbb{Z}$, irreducible = prime
- In $\mathbb{Z}_6$, 2 is prime but not irreducible since $2 = 2 \cdot 4$.

(So for general commutative rings, "prime $\not\Rightarrow$ irreducible".)

Prop In terms of principal ideals, we have

1) $a \mid b$ iff $\langle b \rangle \subseteq \langle a \rangle$
2) $a \sim b$ iff $\langle a \rangle = \langle b \rangle$
3) $u \in R^\times$ iff $\langle u \rangle = R$
4) $a \in R$ is prime iff $\langle a \rangle$ is a prime ideal
5) For an integral domain D,
   $a \in D$ is irreducible iff $\langle a \rangle$ is maximal among the proper principal ideals.

Pf: For 1), note that $a \mid b \Leftrightarrow b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$;

2) follows from 1); 3) & 4) follow from definitions & prev. results.
(how?)

To prove 5), suppose $a \in D$ is irreducible. Then

$$\langle a \rangle \subsetneq \langle b \rangle \subset D \iff b \mid a \text{ and } a \nmid b$$
$$\iff \exists\, c \in D \text{ s.t. } a = bc \;\&\; c \notin D^\times$$
$$\implies b \in D^\times$$

So $\langle a \rangle$ is maximal among principal ideals.

Conversely, suppose $\langle a \rangle$ is maximal among principal ideals.

If $a = bc$, then $\langle a \rangle \subset \langle b \rangle \subset D$ and $\langle a \rangle \subset \langle c \rangle \subset D$

For the former case, maximality implies either $\langle a \rangle = \langle b \rangle$ or $\langle b \rangle = D$. If $\langle b \rangle = D$, then $b \in D^\times$ and we are done.

If $\langle a \rangle = \langle b \rangle$, then $a \sim b \Rightarrow c \in D^\times$ and we are done.

Similar arguments apply for the latter case. #

only place where we need D be an integral domain

Prop 1. Suppose that D is an integral domain. Then every prime is irreducible.

2. If D is a PID, then prime = irreducible.

Pf: 1. Let $a \in D$ be a prime. Suppose that $a = bc$.

Then $a \mid b$ or $a \mid c$.

$\because D$ is a domain

$$a \mid b \Rightarrow b = ar \Rightarrow a = arc \Rightarrow rc = 1 \Rightarrow c \in R^\times$$

Similarly, $a \mid c \Rightarrow b \in R^\times$. Hence a is irreducible.

2. Suppose that a is an irreducible in a PID D.

By 5) in prev. prop., $\langle a \rangle$ is a maximal ideal in D.

In particular, $\langle a \rangle$ is a prime ideal

and hence a is prime in D. #

Example

$\mathbb{Z}[\sqrt{-5}] := \{ a+b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$ is an integral domain as it is a subring of $\mathbb{C}$.

However, 3 is irreducible (we'll see how to show this later)

while $3 \mid 9 = (2+\sqrt{-5})(2-\sqrt{-5})$ & $3 \nmid (2 \pm \sqrt{-5})$

$\Rightarrow \quad 3 \in \mathbb{Z}[\sqrt{-5}]$ is not prime.

Hence in general, even for integral domains, "irreducible $\not\Rightarrow$ prime."

UFD

Def: An integral domain D is called a unique factorization domain (UFD) if

1. Every $a \in D \setminus (D^\times \cup \{0\})$ is a product of irreducibles (Existence)
2. Suppose $c_1 c_2 \cdots c_n = a = d_1 d_2 \cdots d_m$ are two factorizations of a into irreducibles. Then $n = m$ and up to a reordering of factors, $c_i \sim d_i$ for $i = 1, \dots, n$. (Uniqueness)

Examples
- $\mathbb{Z}$ is a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is not a UFD: $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$
  (Later, we'll see that $2, 3, 1 \pm \sqrt{-5}$ are irreducibles in $\mathbb{Z}[\sqrt{-5}]$.)

Rmk In a UFD, irreducible = prime.

Our goal is to show that every PID is a UFD.

Lemma: Let D be a PID. Let

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$$

be an ascending chain of ideals in D. Then $\exists\, n \in \mathbb{Z}_+$ s.t. $\langle a_i \rangle = \langle a_n \rangle \ \forall\, i \geq n$

Rmk: This property is called the ascending chain conditions for principal ideals (ACCPI), and is satisfied by a UFD. (why?)

Pf: Note that $I = \bigcup_i \langle a_i \rangle$ is an ideal in D.

Since D is a PID, $I = \langle b \rangle$ for some $b \in D$.

But $b \in I \Rightarrow b \in \langle a_n \rangle$ for some $n \in \mathbb{Z}_+$.

So for $i \geq n$, $\langle b \rangle \subset \langle a_n \rangle \subset \langle a_i \rangle \subset I = \langle b \rangle$

$\Longrightarrow \langle a_i \rangle = \langle a_n \rangle \ \forall\, i \geq n$. #

Thm Every PID is a UFD.

Pf: (Existence) Let $a \in D \setminus (D^\times \cup \{0\})$.

Suppose that a is not an irreducible. Then

$$a = a_1 b_1$$

where $a_1, b_1 \in D \setminus (D^\times \cup \{0\})$. So we have

$$\langle a \rangle \subsetneqq \langle a_1 \rangle.$$

If a_1 (or b_1) is an irreducible, we stop. Otherwise

$$a_1 = a_2 b_2$$

where $a_2, b_2 \in D \setminus (D^\times \cup \{0\})$. So we have

$$\langle a \rangle \subsetneqq \langle a_1 \rangle \subsetneqq \langle a_2 \rangle.$$

Continuing the same process, we will either get an irreducible a_n dividing a or a strictly ascending chain of ideals $\langle a\rangle \subsetneqq \langle a_1\rangle \subsetneqq \langle a_2\rangle \subsetneqq \cdots$

The latter condition is impossible by the ACCPI.

Hence, for any $a \in D \setminus (D^\times \cup \{0\})$ which is not irreducible, $\exists$ an irreducible $p_1 \in D$ s.t.

$$a = p_1 b_1.$$

Again we have $\langle a\rangle \subsetneqq \langle b_1\rangle$.

If b_1 is not irreducible, then $\exists$ an irreducible $p_2 \in D$

s.t. $b_1 = p_2 b_2$ (so that $a = p_1 p_2 b_2$)

$\Rightarrow \langle a\rangle \subsetneqq \langle b_1\rangle \subsetneqq \langle b_2\rangle$.

Continuing, we get $\langle a \rangle \subsetneqq \langle b_1 \rangle \subsetneqq \langle b_2 \rangle \subsetneqq \cdots$
which must terminate, by ACCPI, say at $\langle b_n \rangle$.
So $a = p_1 p_2 \cdots p_n b_n$ is a factorization into irreducibles.

(Uniqueness) If $p_1 p_2 \cdots p_n = a = q_1 q_2 \cdots q_m$ are two factorizations of $a \in D \setminus (D^\times \cup \{0\})$ into irreducibles (WLOG assume $m \geq n$),

$$\Rightarrow \quad p_1 \mid q_1 q_2 \cdots q_m$$

But irreducibles are primes in a PID,
so $p_1 \mid q_j$ for some $j \in \{1, \ldots, m\}$.

Up to a permutation we can assume $j = 1$.

Then $q_1 = p_1 u_1$ where $u_1 \in D^\times$.

So $$p_1 p_2 \cdots p_n = p_1 u_1 q_2 \cdots q_m$$
$$\Longrightarrow \quad p_2 \cdots p_n = u_1 q_2 \cdots q_m$$
Now $p_2 \mid u_1 q_2 \cdots q_m \Rightarrow p_2 \mid q_j$ for some $j \in \{2, \ldots, m\}$ ($p_2 \nmid u_1$ since p_2 is not a unit). Up to a permutation we can assume $j=2$.
Then $q_2 = p_2 u_2$ for some $u_2 \in D^\times$. So
$$p_2 \cdots p_n = u_2 p_2 q_3 \cdots q_m$$
$$\Longrightarrow \quad p_3 \cdots p_n = u_2 q_3 \cdots q_m.$$
Continuing this process, we end up with $q_i = p_i u_i$ for $i = 1, \ldots, n$

and $\quad 1 = u_1 \cdots u_n q_{n+1} \cdots q_m$

But then we must have $m=n$ since $q_i \notin D^\times$. #

Rmks 1) In fact we have proved

ACCPI $\Rightarrow$ existence, and

"prime = irreducible" $\Rightarrow$ uniqueness.

So altogether we have:

An integral domain D is a UFD iff

(i) ACCPI holds and

(ii) "prime = irreducible".

Examples Since $\mathbb{Z}$, $F[x]$ are PIDs, they are UFDs.

Euclidean domains

More examples of UFDs are given by the following:

Def An Euclidean norm on an integral domain D is a function
$$N : D\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0} \text{ satisfying}$$

1. $\forall\, a,b \in D$ with $b \neq 0$, $\exists\, q,r \in D$ s.t. $a = bq + r$ where either $r = 0$ or $N(r) < N(b)$. (divison algorithm)
2. $\forall\, a,b \in D\setminus\{0\}$, $N(a) \leq N(ab)$.

An Euclidean domain is an integral domain w/ an Euclidean norm.

<u>Examples</u>
- $\mathbb{Z}$ w/ $N(a) := |a|$
- $F[x]$ w/ $N(f) := \deg f$

<u>Prop</u> Every Euclidean domain is a PID, and hence a UFD.

<u>Pf</u>: By divison algorithm, any ideal I is generated by an element $a \in I$ with minimum value of N. #

Gaussian integers

Consider $\mathbb{Z}[i] := \{a+bi \mid a, b \in \mathbb{Z}\}$.

For any $\alpha = a+bi \in \mathbb{Z}[i]$, define $N(\alpha) = a^2+b^2$.

Prop $\mathbb{Z}[i]$ equipped w/ N is an Euclidean domain.

Pf: Since $\mathbb{Z}[i]$ is a subring in $\mathbb{C}$, it is an integral domain.

Note that $\alpha \neq 0 \Rightarrow N(\alpha) \geq 1$ & $N(\alpha\beta) = N(\alpha)N(\beta)$ $\forall \alpha, \beta$.

So $\forall \alpha, \beta \neq 0$, $N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta)$.

Now let $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i \neq 0$

Let $b := N(\beta) = b_1^2 + b_2^2 > 0$. Write $\alpha\bar{\beta} = c_1 + c_2 i$.

By division algorithm in $\mathbb{Z}$, $\exists\, q_1, q_2, r_1, r_2 \in \mathbb{Z}$

s.t. $\begin{cases} c_1 = q_1 b + r_1 \\ c_2 = q_2 b + r_2 \end{cases}$ where $|r_i| \leq \frac{b}{2}$

Then

$$\alpha\bar{\beta} = qb + r_0 \quad \text{where } q := q_1 + q_2 i,\ r_0 = r_1 + r_2 i.$$

and $N(r_0) = r_1^2 + r_2^2 \leq \frac{b^2}{2} < b^2 = N(\beta\bar{\beta})$.

Let $r := \alpha - q\beta$. Then $\alpha = q\beta + r$ where either $r = 0$ or $N(r) < N(\beta)$. #

Thm (Fermat) Let p be an odd prime in $\mathbb{Z}$. Then $\exists\, a, b \in \mathbb{Z}$ s.t. $p = a^2 + b^2$ iff $p \equiv 1 \pmod 4$

Pf: ($\Longrightarrow$) straightforward (a, b cannot be both even or both odd).

($\Longleftarrow$) Suppose that $p \equiv 1 \pmod 4$.

Now $\mathbb{Z}_p^\times$ is cyclic & $4 \mid (p-1) = |\mathbb{Z}_p^\times|$

$\Longrightarrow \exists\, n \in \mathbb{Z}_p^\times$ with multiplicative order 4.

So $n^2 \equiv -1 \pmod p$, i.e. $p \mid n^2+1$ in $\mathbb{Z}$.

In $\mathbb{Z}[i]$,

$$p \mid n^2+1 = (n+i)(n-i).$$

This implies that p is reducible in $\mathbb{Z}[i]$ since $p \nmid n \pm i$.

Hence $p = (a+bi)(c+di)$ in $\mathbb{Z}[i]$

where $a+bi$, $c+di$ are not units, so $\underset{\underset{N(a+bi)}{\|}}{a^2+b^2}, \underset{\underset{N(c+di)}{\|}}{c^2+d^2} > 1$

$\alpha \in \mathbb{Z}[i]$ is a unit $\Longleftrightarrow N(\alpha) = 1$ since N is multiplicative.

$$\Longrightarrow \quad p^2 = (a^2+b^2)(c^2+d^2)$$

$$\Longrightarrow \quad p = a^2+b^2 = c^2+d^2. \quad \#$$

Another example

Consider $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. This is an integral domain.

For $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, let $N(\alpha) := a^2 + 5b^2$. Then

$$\begin{cases} N(\alpha) = 0 \iff \alpha = 0 \\ N(\alpha\beta) = N(\alpha)N(\beta) \quad \forall \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]. \end{cases}$$

Now $\boxed{2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})}$ in $\mathbb{Z}[\sqrt{-5}]$.

Note that $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit $\iff N(\alpha) = 1 \iff \alpha = \pm 1$.

3 is irreducible: Suppose $3 = \alpha\beta$ where both α, β are non-units.

Then $9 = N(3) = N(\alpha)N(\beta) \Rightarrow N(\alpha) = N(\beta) = 3$.

But $a^2 + 5b^2 = 3$ has no solutions in $\mathbb{Z}$ ($a^2 \equiv 3 \pmod 5$ has no solutions).

Similarly, $2, 1 \pm \sqrt{-5}$ are all irreducibles, and $3 \nsim 1 \pm \sqrt{-5}$.

So $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

A theorem of Gauss

Let D be a UFD. Consider the polynomial ring $D[x]$.

Def For $0 \neq f = a_0 + a_1 x + \dots + a_n x^n \in D[x]$, we define the content of f (denoted by $c(f)$) to be $\gcd(a_0, a_1, \dots, a_n)$ (which is well-defined up to multiplication by units).

f is called primitive if $c(f) \sim 1$.

Lemma (Gauss' Lemma) The product of two primitive polynomials in $D[x]$ remains primitive.

Pf: Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + b_1 x + \dots + b_m x^m$ be primitive in $D[x]$.

Let p be an irreducible in D.

$\exists\, r, s$ s.t. $\begin{cases} p \mid a_i \text{ for } i<r \ \& \ p \nmid a_r \\ p \mid b_j \text{ for } j<s \ \& \ p \nmid b_s \end{cases}$

Now the coefficient of x^{r+s} in $h(x) := f(x)\,g(x)$ is given by

$$c_{r+s} := \underbrace{(a_0 b_{r+s} + \dots + a_{r-1} b_{s+1})}_{\text{divisible by } p} + \underbrace{a_r b_s}_{\text{not divisible by } p} + \underbrace{(a_{r+1} b_{s-1} + \dots + a_{r+s} b_0)}_{\text{divisible by } p}$$

$\Longrightarrow \quad p \nmid c_{r+s}$. #

Lemma Let F be a field of quotients of D, and $f(x) \in D[x]$. Then

(i) $f(x)$ is irreducible in $D[x] \Rightarrow f(x)$ is also irreducible in $F[x]$.

(ii) $f(x)$ is primitive in $D[x]$ & irreducible in $F[x] \Rightarrow f(x)$ is irreducible in $D[x]$.

Pf: (i) Suppose that $f(x) \in D[x]$ factors into lower degree polynomials in $F[x]$: $\quad f = gh \quad , \quad g, h \in F[x]$.

By clearing denominators, we have

$$df = g_1 h_1 \quad \text{for some } d \in D \ \& \ g_1, h_1 \in D[x]$$

We can write $f = c\tilde{f}$, $g_1 = c_1 g_2$, $h_1 = c_2 h_2$

where $c, c_1, c_2 \in D$ and $\tilde{f}, g_2, h_2$ are primitive in $D[x]$.

Then $dc\tilde{f} = c_1 c_2 g_2 h_2$. Taking contents on both sides, we have $dc \sim c_1 c_2$. Hence $\exists u \in D^\times$ s.t. $c_1 c_2 = udc$.

$\Longrightarrow f = ucg_2 h_2$. In particular, f is reducible in $D[x]$.

(ii) f is reducible & primitive in $D[x] \Rightarrow \exists g, h$ w/ $\deg g, \deg h < \deg f$ s.t. $f = gh \Rightarrow f$ is reducible in $F[x]$. #

Thm (Gauss) If D is a UFD, then $D[x]$ is a UFD.

Pf: (Existence) Let $0 \neq f \in D[x]$. If $\deg f = 0$, then $f \in D \setminus \{0\}$. Since D is a UFD, either $f \in D^\times$ or f factorizes into a product of irreducibles. But irreducibles in D are irreducibles in $D[x]$.

So assume $\deg f \geq 1$. Write f as $c(f) f_1$ where f_1 is primitive. It suffices to show that f_1 factors into a product of irreducibles. Let F be a field of quotients of D. Regard $f_1 \in F[x]$.

Since $F[x]$ is a PID and hence a UFD,

$$f_1 = q_1 \cdots q_n$$

where $q_1, \dots, q_n$ are irreducibles in $F[x]$.

Write
$$q_i = \frac{a_i}{b_i} p_i$$
where $0 \neq a_i, b_i$ and p_i is primitive in $D[x]$.

By (ii) in the above lemma, p_i is irreducible in $D[x]$.

Now $$b f_1 = a p_1 \cdots p_n \quad \text{where } b = \prod_i b_i, \ a = \prod_i a_i.$$

Since f_1 and $p_1 \cdots p_n$ are primitive (by Gauss Lemma), by taking content, we get
$$f_1 = u p_1 \cdots p_n \quad \text{where } u \in D^\times.$$

Hence f_1 is a product of irreducibles in $D[x]$.

(Uniqueness) Let $0 \neq f \in D[x]$ be a non-unit. If $\deg f = 0$, then uniqueness follows from the fact that D is a UFD.

So assume $\deg f \geq 1$.

If $\quad c_1 \cdots c_r p_1 \cdots p_n = f = d_1 \cdots d_s q_1 \cdots q_m$

are two factorizations of f w/ $c_1, \dots, c_r, d_1, \dots, d_s \in D$

and $\deg p_i, \deg q_j \geq 1$, then

$$c_1 \cdots c_r \sim c(f) \sim d_1 \cdots d_s$$

Now D is a UFD $\Rightarrow$ $r = s$ and $c_i \sim d_i$ (up to permutation)

So $\quad p_1 \cdots p_n = u q_1 \cdots q_m \quad , u \in D^\times$.

By (i) of above lemma, p_i's & q_j's are irreducibles in $F[x]$.

Now $F[x]$ is a UFD $\Rightarrow$ $n = m$ and $p_i \sim q_i$ in $F[x]$ (up to permutation)

i.e. $\exists\, a_i, b_i \in D \setminus \{0\}$ s.t. $\quad a_i p_i = b_i q_i$

Since p_i, q_i are primitive, taking contents again shows that

$p_i \sim q_i$ in $D[x]$. #

Cor If D is a UFD, then $D[x_1,\dots,x_n]$ is a UFD.

Pf: Note that $D[x_1,\dots,x_n] = D[x_1,\dots,x_{n-1}][x_n]$. #

Rmk However $D[x_1,\dots,x_n]$ is not a PID for $n \geq 2$ since the ideal $\langle x_1,\dots,x_n \rangle$ is not principal.