Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 17, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Factorization

0.1.1 Factorization of Integers and Polynomials

Now we are going to discuss some of the nice properties of the integers with regards to factorization. One of the most important ones is that for any a, b with $a \neq 0$ there are q, r such that

Properties of the Integers

- $b = aq + r$
- $0 \leq r < |a|$

From this fact we get several important results. Including

Theorem 0.1.1.1. *If a, b have no factor in common other than ± 1 then there are c, d such that $ac + bd = 1$*

and

Theorem 0.1.1.2. *Let p be a prime integer and let a, b be integers. Then if p divides ab we must have p divides a or p divides b.*

Which will get us

$$\boxed{\textbf{Fundamental Theorem of Arithmetic}}$$

Theorem 0.1.1.3 (Fundamental Theorem of Arithmetic)**.** *Every integer $a \neq 0$ can be written as a product*

$$a = cp_1 \cdots p_k$$

where c is ± 1 and each p_i is prime. And further, up to the ordering this product is unique.

Proof. First we need to show a prime factorization exists. It suffices to consider the case when $a > 1$. And, we can assume that this is the case for all $b < a$.

Now there are two cases

Case 1: a is prime. Then we are done.

Case 2: $a = bb'$. then both b, b' are less than a and hence have a prime factorization.

Next we need to show that prime factorizations are unique. Let

$$\pm p_1 \dots p_n = \pm q_1 \dots q_m$$

where all p_i, q_j are prime. We use the fact that if p divides ab then p divides a or p divides b. This means that for each p_1, p_i must divide some q_i. Hence, because q_i is prime $p_1 = q_i$ for some i. We can then cancel p_1 from both sides and proceed by induction. □

Polynomial Rings over Fields

Theorem 0.1.1.4. *Let F be a field and let $F[x]$ denote the polynomial ring in one variable over F.*

(a) *If two polynomials f, g have no common non-constant factor then there are polynomials $r, s \in F[x]$ such that $rf + sg = 1$*

(b) *If an irreducible polynomial $p \in F[x]$ divides a product fg then p divides one of the factors.*

(c) *Every nonzero polynomial $f \in F[x]$ can be written as a product*

$$cp_1 \cdots p_n$$

where c is a nonzero constant and the p_i are monic irreducible polynomials in $F[x]$ and $n \geq 0$. This factorization is unique except for the ordering of the terms.

Proof. *********PROVE (B) (MAYBE) MAYBE GIVE (A), (C) AS HOMEWORK (ASSUMING (B)) Same as the case for integers. MAYBE PROVE THIS INSTEAD OF THE INTEGER CASE ********* □

Similarly we have

Number of Roots of a Polynomial

Theorem 0.1.1.5. *Let F be a field and let $f(x)$ be a polynomial of degree n with coefficients in F. Then f has at most n roots in F.*

Proof. An element $\alpha \in F$ is a rot of f if and only if $(x - \alpha)$ divides f. So if we can then write $f(x) = (x - \alpha)q(x)$ where $q(x)$ is a polynomial of degree $n - 1$. If β is another root of f then $f(\beta) = (\beta - \alpha)q(\beta) = 0$ and so β is a root of $q(x)$ (as the product of non-zero elements is non-zero in a field). Hence by induction on n we see that f has at most n rots. □

0.2 Unique Factorization Domains, Principle Ideal Domains, and Euclidean Domains

Now that we have have seen that the integers and polynomials rings over fields behave similarly it is natural to ask which other rings behave in a similar manner. So that we have the cancellation law we will assume that all of these rings are integral domains.

Divisors, Irreducible Elements, Associates

Definition 0.2.0.6. Let R be an integral domain. If $a, b \in R$ we say that a divides b if $(\exists r \in R) ar = b$.

We say that a is a proper divisor of b if $b = qa$ for some $q \in R$ and neither q nor a is a unit.

We say a non-zero element a of R is irreducible if it is not a unit and if it has no proper divisor.

We say that $a, a' \in R$ are associates if a divides a' and a' divides a. It is easy to show that if a, a' are associates then $a = ua'$ for some unit $u \in R$.

We can think of these ideas in terms of the principle ideals which they generate.

Connections to Ideals

Theorem 0.2.0.7.

$$\begin{aligned} u \textit{ is a unit} \quad &\Leftrightarrow (u) = (1) \\ a \textit{ and } a' \textit{ are associates} \quad &\Leftrightarrow (a) = (a') \\ a \textit{ divides } b \quad &\Leftrightarrow (a) \supset (b) \\ a \textit{ is a proper divisor of } b \quad &\Leftrightarrow (1) > (a) > (b) \end{aligned}$$

Proof. Immediate. □

We then have the following result which compares the process of factoring with ideas.

Factorization and Chains of Ideals

Theorem 0.2.0.8. *Let R be an integral domain. Then the following are equivalent*

(a) For every non-zero element $a \in R$ which is not a

unit factors as

$$a = b_1 \dots b_n$$

where each b_i is irreducible.

(b) R does not contain an infinite increasing chain of principle ideals

$$(a_1) < (a_2) < (a_3) < \cdots$$

Proof. Suppose R contains an infinite increasing sequence

$$(a_1) < (a_2) < (a_3) < \cdots$$

Then $(a_n) < (1)$ for all n because $(a_n) < (a_{n+1}) \subseteq (1)$. Since $(a_{n-1}) < (a_n)$, a_n is a proper divisor of a_{n-1}. Say $a_{n-1} = a_n b_n$ where $a_n b_n$ are not units. This provides a non-terminating sequence of factorizations $a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2 \dots$. Conversely such a factorization gives us an increasing chain of ideals. □

We call these conditions either the ascending chain condition for princip or that existence of factorizations holds in R.

0.2.1 Examples

Non-UFD To see an example of when the existence of factorization fails consider the following ring

$$F[x_1, x_2, \dots]/(x_2^2 - x_1, x_3^2 - x_2, \dots)$$

This ring is essentially F with $x^{2^{-k}}$ adjoined for each $k \in \omega$. I.e. we adjoin the equations $x_{i+1}^2 = x_i$

This doesn't have the ascending chain condition because we see that

$$(x_1) < (x_2) < \dots$$

is an infinite ascending chain of principle ideals.

0.2.2 Unique Factorization Domains

Unique Factorization Domains

Definition 0.2.2.1. We say that an integral domain R is a Unique Factorization Domain (UFD) if

(i) Existence of factors is true for R.

(ii) If $a \in R$ and $a = p_1 \dots p_n$ and $a = q_1 \dots q_m$ where p_i, q_j are all irreducible, then $m = n$ and with a suitable ordering p_i and q_i are associates for each i.

To see how this can fail consider $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. We then have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and it isn't hard to show that $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are all irreducible. But because ±1 are the only units it is also clear that these are not associates of each other.

Hence $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

The crucial property of primes which we use in UFD's is $\boxed{\textbf{Prime Elements}}$

Definition 0.2.2.2. Let R be an integral domain. We say that $p \in R$ is prime if $p \neq 0$ and for all $ab \in R$ such that p divides ab, either p divides a or p divides b.

Theorem 0.2.2.3. *Let R be an integral domain. Suppose existence of factorization holds in R. Then R is a UFD if and only if every irreducible element is prime.*

Proof. ********Proposition 11.2.8 MAYBE GIVE AS HOMEWORK ******** □

Theorem 0.2.2.4. *Let R be a UFD and let $a = p_1 \ldots p_n$ and let $b = q_1 \ldots q_m$ be prime factorizations of a and b. Then a divides b if and only if $m \geq n$ and under a suitable ordering of the factors q_i of b, p_i is an associate of q_i for all $i \leq n$*

Proof. Immediate □

Greatest Common Divisors in UFD's

Corollary 0.2.2.5. *Let R be a UFD and let $a, b \in R$ where we don't have both $a = 0$ and $b = 0$. Then there exists a greatest common divisor d of a, b with the following properties*

(i) d divides a and b

(ii) if an element e of R divides a and b then e divides d

It follows form the definition that any two greatest common divisors are associate, but a greatest common divisor does not need to be of the form $aq + bp$.

For example $\mathbb{Z}[x]$ is a UFD and $2, x$ have a greatest common divisor of 1 but 1 is not a linear combination of 2 and x with integer coefficients.

0.2.3 Principle Ideal Domains

Principle Ideal Domains

Definition 0.2.3.1. We say an integral domain R is a Principle Ideal Domain (PID) if every ideal is principle.

Theorem 0.2.3.2. *(a) In an integral domain, a prime element is irreducible.*

(b) In a PID an irreducible element is prime.

Proof. ********Proposition 11.2.11 MAYBE GIVE AS HOMEWORK ******** □

PID implies UFD

Theorem 0.2.3.3. *A Principle Ideal Domain is a Unique Factorization Domain.*

Proof. Suppose that R is a PID. Then every irreducible element of R is prime. So we only need to prove the existence of factorizations for R (and uniqueness is taken care of).

We have shown that this is equivalent to there being no infinite ascending chain. We will argue by contradiction so lets assume that

$$(a_1) < (a_2) < \cdots$$

is such a chain

Lemma 0.2.3.4. *Let R be any ring. The union of an increasing chain of ideals*

$$I_1 \subset I_2 \subset \dots$$

is an ideal.

Proof. Let

$$I = \bigcup_{n \in \omega} I_n$$

. If $u, v \in I$ then $u, v \in I_n$ for some I_n and so $u + v \in I_n \subseteq I$. □

Let

$$A = \bigcup_{n \in \omega} (a_n)$$

. Then A is an ideal and in particular $A = (b)$ for some $b \in R$ as R is a PID. But then there must be some n such that $b \in (a_n)$.

But then we have $(a_n) \subset (a_{n+j}) \subset A = (b) \subseteq (a_n)$. So we have $(a_n) = (a_{n+j})$ for all j contradicting that $(a_1) < (a_2) < \ldots$ was an infinite ascending chain. □

Note however that there are unique factorization domains which are not principle ideal domains (like $\mathbb{Z}[x]$).

PID's and M

Theorem 0.2.3.5. *(a) Let p be a nonzero element of a principle ideal domain R. Then $R/(p)$ is a field if and only if p is irreducible.*

(b) The maximal ideals are the principle ideals gen-

erated by irreducible elements.

Proof. Since an ideal M is maximal if and only if R/M is a field then the two parts are equivalent. So we will prove the second part.

We will prove part (a). $(a) \supseteq (b)$ if and only if a divides b. The only divisors of an irreducible element p are the unites and the associates of p. Therefore the only principle ideals which contain (p) are (p) and (1). Since every ideal of R is principle this shows that an irreducible element generates a maximal ideal.

Conversely let $b = aq$ where neither a nor q are a unit. Then we have $(b) < (a) < (1)$ and so (b) is not maximal. □

0.2.4 Euclidean Domains

The next step we want to take is to generalize the division with remainder procedure. Now in order to do this we need a sense of size in a ring. Recall that for the following rings we have the following sizes

$$\begin{aligned} \text{absolute value if } \; R = & \; \mathbb{Z} \\ \text{degree of a polynomial if } \; R = & \; F[x] \\ (\text{absolute value})^2 \; R = & \; \mathbb{Z}[i] \end{aligned}$$

So in particular we have a the following definition **Euclidian Do**

Definition 0.2.4.1. Let R be an integral domain. We say that R is a Euclidean Domain if there is a size function

$$\sigma : R - \{0\} \to \{0, 1, 2, \dots\}$$

Such that if $a, b \in R$ and $a \neq 0$ then there are $p, q \in R$

with

$$b = aq + r$$

and either $r = 0$ or $\sigma(r) < \sigma(a)$

As examples we have $\mathbb{Z}, F[x], \mathbb{Z}[i]$ are Euclidean Domains.

Theorem 0.2.4.2. *A Euclidean Domain is a principle ideal domain and hence also a unique factorization domain.*

Proof. ********Proposition 11.2.20. MAYBE GIVE AS HOMEWORK OR SAY IS IMMEDIATE. ******** □

0.3 Gauss's Lemma

We know that $\mathbb{Q}$ is a field and hence we also know that $\mathbb{Q}[x]$ is a unique factorization domain. So in particular, given any polynomial $p(x) \in \mathbb{Z}(x)$ we know that it can be factored in $\mathbb{Q}[x]$. But we can then ask the question, "Can this factorization be done inside $\mathbb{Z}[x]$?". The answer is

YES and that is what we will now prove.

Primitive Polynomials

Definition 0.3.0.3. A polynomial $\Sigma_i a_i x^i \in \mathbb{Z}[x]$ is called primitive if $gcd(a_1, \ldots, a_n) = 1$ and $_n$ is positive.

Primitive Decomposition of Polynomials

Theorem 0.3.0.4. *Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as the product*

$$f(x) = cf_0(x)$$

where c is a rational number (called the <u>content</u> of $f(x)$) and $f_0(x) \in \mathbb{Z}[x]$ and is primitive.

Further the polynomial f has integer coefficients if and only if c is an integer.

Proof. First what we do is factor out all the denominators to get a polynomial $f_1 \in \mathbb{Z}[x]$ such that $f(x) = \frac{1}{n} f_1(x)$

for some $n \in \mathbb{Z}$. Then factor out the greatest common divisor of the coefficients of f_1 to get a polynomial f_0 where $f_1(x) = c * f_0(x)$. This proves existence.

To show uniqueness lets assume we have $cf_0(x) = dg_0(x)$ where $f_0(x), g_0(x)$ are primitive. We then want to show that $c = d$ and $f_0(x) = g_0(x)$.

By cross multiplication it suffices to consider the case when c, d are integers.

Let $\{a_i\}, \{b_i\}$ be the coefficients of $f_0(x), g_0(x)$ respectively. We therefore have that $ca_i = db_i$ for all i. But we also have that $gcd\{a_i\}gcd\{b_i\} = 1$. Hence $gcd\{ca_i\} = c$ and $gcd\{db_i\} = d$ and we have $c = \pm d$ and $f_0 = \pm g_0$. But because the leading coefficient of f_0 and of g_0 are positive this means that $c = d$ and $f_0 = g_0$. $\square$

Gauss's Lemma

Theorem 0.3.0.5 (Gauss's Lemma)**.** *A product of primitive polynomials in $\mathbb{Z}[x]$ is primitive*

Proof. Let $f, g \in \mathbb{Z}[x]$ be primitive and let $h = fg$. We know that the leading coefficient of h is positive as the leading coefficient of g and f are.

We will show that no prime p divides all the coefficients of $h(x)$. This will show that the gcd of the coefficients of h is 1 and hence that h is primitive.

Consider the homomorphism $\varphi_p : \mathbb{Z}[x] \to \mathcal{F}_p[x]$. If we can show that $\varphi_p(h) \neq 0$ then we are done. But we know that $\varphi_p(f) \neq 0$ and $\varphi_p(g) \neq 0$ because f, g are primitive and hence the gcd of their coefficients is 1. But, $\mathcal{F}_p$ is an integral domain and we have $\varphi_p(h) = \varphi_p(f) \cdot \varphi_p(g)$ and so $\varphi_p(h) \neq 0$. □

Theorem 0.3.0.6. *(a) Let f, g be polynomials in $\mathbb{Q}[x]$ and let f_0, g_0 be the associated primitive polynomials in $\mathbb{Z}[x]$ If f divides g in $\mathbb{Q}[x]$ then f_0 divides g_0 in $\mathbb{Z}[x]$*

(b) Let f be a primitive polynomial in $\mathbb{Z}[x]$ and let g be any polynomial with integer coefficients. Suppose that f divides g in $\mathbb{Q}[x]$, say $g = fq$ with $q \in \mathbb{Q}[x]$. Then $q \in \mathbb{Z}[x]$ and hence f divides g in $\mathbb{Z}[x]$

(c) Let f, g be polynomials in $\mathbb{Z}[x]$. If they have a common nonconstant factor in $\mathbb{Q}[x]$, then they have a common nonconstant factor in $\mathbb{Z}[x]$ too.

Proof. To prove (a) clear denominators so that f, g become primitive and then (a) is a consequence of (b).

In order to prove (b) we apply the previous theorem to get $q = cq_0$ where $c \in \mathbb{Q}$ and q_0 is primitive. We then have fq_0 is primitive and $g = cfq_0$ shows that $fq_0 = g_0$ the primitive polynomial associated to g and $g = cg_0$. But as $g \in \mathbb{Z}[x]$ this means that $c \in \mathbb{Z}$ and hence $q \in \mathbb{Z}[x]$.

To prove c suppose that f, g have a common factor h. We may assume that h is primitive (as we are working in $\mathbb{Q}[x]$ and if h divides f, g then so does ch). But then by part (b) we have that h divides f, g in $\mathbb{Z}[x]$ □

Corollary 0.3.0.7. *If a nonconstant polynomial f is irreducible in $\mathbb{Z}[x]$ then it is irreducible in $\mathbb{Q}[x]$*

Proof. Immediate □

Irreducibility in $\mathbb{Z}[x]$

Theorem 0.3.0.8. *Let f be an integer polynomial with positive leading coefficient. Then f is irreducible* *in $\mathbb{Z}[x]$ if and only if either*

(a) f is a prime integer or

(b) f is a primitive polynomial which is irreducible in $\mathbb{Q}[x]$

Proof. Suppose f is irreducible. We ay write $f = cf_0$ where f_0 is primitive. Since f is irreducible this can't be a proper factorization so either $f_0 = 1$ or $c = 1$. □

Theorem 0.3.0.9. *Every irreducible element of $\mathbb{Z}[x]$ is a prime element*

Proof. Let f be irreducible and suppose f divides gh where $gh \in \mathbb{Z}[x]$.

Case 1: $f = p$ a prime integer. Let $g = cg_0$ and $h = h_0$ where g_0, h_0 are primitive. We have that g_0h_0 is also primitive. So in particular there is some coefficient a which is not divisible by p. But we have p divides gh

so p divides cda. And in particular this means that p divides c or p divides d. Hence p divides g or p divides h.

Case 2: f is a primitive polynomial which is irreducible in $\mathbb{Q}[x]$. We then have f is a prime element of $\mathbb{Q}[x]$ and so f divides g or f divides f in $\mathbb{Q}[x]$. Hence f divides g or f divides h in $\mathbb{Z}[x]$. □

Theorem 0.3.0.10. *The polynomial ring $\mathbb{Z}[x]$ is a unique factorization domain. Every nonzero polynomial $f(x) \in \mathbb{Z}[x]$ which is not ± 1 can be written as the product*

$$f(x) = \pm p_1 \dots p_m q_1(x) \dots q_n(x)$$

where the p_i are prime integers and the $q_i(x)$ are irreducible primitive polynomials. This expression is unique up to rearrangement of factors.

Proof. Immediate □

Now if we let R be any UFD and let F be the field of fractions of R then the results above can be copied (we just have to allow some ambiguity to deal with units). Specifically we have

Generalization to Arbitrary UFD's

Theorem 0.3.0.11. *Let R be a unique factorization domain with field of fractions F*

(a) Let f, g be polynomials in $F[x]$ and let f_0, g_0 be the associated primitive polynomials in $R[x]$. If f divides g in $F[x]$ then f_0 divides g_0 in $R[x]$

(b) Let f be a primitive polynomial in $R[x]$, and let g be any polynomial in $R[x]$. Suppose that f divides g in $F[x]$, say $g = fq$ with $q \in F[x]$. Then $q \in R[x]$ and hence f divides g in $R[x]$.

(c) Let f, g be polynomials in $R[x]$. If they have a

common nonconstant factor in $F[x]$ then they have a common nonconstant factor in $R[x]$ also.

(d) If a nonconstant polynomial f is irreducible in $R[x]$ then it is irreducible in $F[x]$ also.

(e) $R[x]$ is a unique factorization domain.

Proof. This follows the previous proofs concerning $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$. □

Corollary 0.3.0.12. *The polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ and $F[x_1, \ldots, x_n]$ where F is a field are unique factorization domains.*

0.4 TODO

- Go through Lang's book on the same topics.