M373K Lecture Notes

Lewis Bowen*
University of Texas at Austin

April 18, 2013

Contents

1 4/16/13: A few reminders

There is a homework due Thurs.

Definition 1. A polynomial $f \in \mathbb{Z}[x]$ is *primitive* if the gcd of its coefficients is 1. More generally, the *content* of $f \in \mathbb{Z}[x]$ is the gcd of its coefficients. So we may write $f = dg$ where $d \in \mathbb{Z}$ is the content of f and q is primitive.

Lemma 1.1. *The product of primitive polynomials is primitive.*

Proof. Let

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0.$$

*email:lpbowen@math.utexas.edu

Let d be the content of fg. To obtain a contradiction suppose $d > 1$. Let p be a prime dividing d. Let $j \geq 0$ be the smallest number such that $p \nmid a_j$ and let $k \geq 0$ be the smallest number such that $p \nmid b_k$. Then the coefficient on x^{j+k} is

$$c_{j+k} = a_j b_k + a_{j+1} b_{k-1} + \cdots a_{j+k} b_0.$$

But notice that $p \mid b_0, b_1, \ldots$. Since also $p \mid c_{j+k}$ we must have $p \mid a_j b_k$ which is impossible. This contradiction implies the lemma. $\square$

Motivation: $2x^2 + 2$ is reducible in $\mathbb{Z}[x]$ because it equals $2(x^2 + 1)$. But it is irreducible in $\mathbb{Q}[x]$.

Theorem 1.2 (Gauss' Lemma)**.** *If a primitive polynomial $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$.*

Proof. Let $f(x) = u(x)v(x)$ where $u, v \in \mathbb{Q}[x]$ have positive degree. By clearing denominators and taking out common factors we can write this as

$$f(x) = \frac{a}{b}\lambda(x)\mu(x)$$

where a, b are coprime integers and $\lambda, \mu \in \mathbb{Z}[x]$ are primitive. So

$$bf(x) = a\lambda(x)\mu(x).$$

The content on the left hand side is b. The content on right hand side is a (because the previous lemma implies that the product $\lambda\mu$ is primitive). So $a = b$ and $f = \lambda\mu$. $\square$

Definition 2. A polynomial in $\mathbb{Z}[x]$ is integer monic if its leading coefficient is 1.

Corollary 1.3. *If an integer monic polynomial factors over $\mathbb{Q}$ then it factors into integer monic polynomials.*

So how do we know when a polynomial is irreducible? here's one criterion:

Lemma 1.4. *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. If p is a prime with $p \nmid a_n$ and the residue of f mod p (for some prime p) is irreducible in $\mathbb{F}_p[x]$ then f is irreducible in $\mathbb{Q}[x]$. In particular, if f is also primitive, then f is irreducible in $\mathbb{Z}[x]$.*

Example: $x^4 - 6x^3 + 12x^2 - 3x + 9$ equals $x^4 + x + 1$ mod 2 which is irreducible (in $\mathbb{F}_2[x]$). So this poly is irreducible in $\mathbb{Z}[x]$.

We will present one criterion due to Eisenstein:

Theorem 1.5 (Eisenstein's criterion)**.** *Let $f(x) = a_n x^n + \cdots + a_0$. Suppose p is a prime, $p \mid a_i$ for all $0 \leq i \leq n-1$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over $\mathbb{Q}$.*

Proof. Wlog f is primitive. To obtain a contradiction, we assume f is reducible. Using Gauss' Lemma, we obtain

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

where the b_i, c_i's are integers. Note $a_0 = b_0 c_0$. Since $p \mid a_0, p^2 \nmid a_0$ we have wlog $p \mid b_0, p \nmid c_0$. There must be a smallest number k such that $p \nmid b_k$ (otherwise $p|a_i$ for all i which is false). Note

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots b_0 c_k.$$

If $k < n$ then $p \mid a_k$ now implies $p \mid b_k c_0$ which is false. So $k = n$. But this also doesn't make sense because it implies that $s = 0$ so we don't really have a factorization after all. $\square$

Example: the polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$. Why? Well, it doesn't satisfy the Eisenstein criterion but if you consider $f(x+1) = (x+1)^{p-1} + \cdots + (x+1) + 1$ and rewrite the coefficients you'll find that it does satisfy the Eisenstein criterion. So $f(x+1)$ is irreducible over $\mathbb{Q}$. But this implies $f(x)$ is irreducible over $\mathbb{Q}$ as well.

2 Polynomial rings over commutative rings

Throughout this section R is a commutative ring with unit.

Recall the definition of $R[x]$ and $R[x_1, \ldots, x_n]$.

Lemma 2.1. *If R is an ID then so is $R[x]$.*

Recall that $R[x, y] = R[x][y]$ for example.

Corollary 2.2. *If R is an ID then so is $R[x_1, x_2, \ldots, x_n]$.*

Recall the definition of UFD and gcd.

Lemma 2.3. *If R is a UFD then any two elements have a gcd.*

Corollary 2.4. *If R is a UFD then every irreducible element is prime (and every prime element is irreducible).*

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

Recall the notion of primitive polynomial and the content of a polynomial.

Lemma 2.5. *If R is a UFD, then any product of primitive polynomials in $R[x]$ is primitive. In fact $c(fg) = c(f)c(g)$.*

We'd like to know if there's a form of Gauss' lemma - that irreducible polynomials of $R[x]$ are still irreducible in $F[x]$ where F is the field of fractions of R.

Lemma 2.6. *If $f \in R[x]$ is primitive and irreducible in $R[x]$ then it is irreducible in $F[x]$.*

Lemma 2.7 (Key Lemma)**.** *Suppose R is a UFD. Any primitive polynomial in $R[x]$ can be factored in a unique way as a product of irreducible polynomials in $R[x]$.*

Proof. This is similar to Gauss' Lemma. Let $f \in R[X]$ be primitive. Because $F[X]$ is a Euclidean ring and therefore a UFD, $f = p_1 \cdots p_n$ for some irreducible polynomials $p_i \in F[X]$. By clearing denominators and factoring out the gcd's we see that $p_i = (a_i/b_i)q_i$ where $a_i, b_i \in R$ and $q_i \in R[X]$ is a primitive irreducible polynomial. Therefore

$$f = \frac{a_1 \cdots a_n}{b_1 \cdots b_n} q_1 \cdots q_n$$

and

$$(b_1 \cdots b_n) f = (a_1 \cdots a_n)(q_1 \cdots q_n).$$

But the content of the LHS is $b_1 \cdots b_n$ and the content of the RHS is $(a_1 \cdots a_n)$. So $a_1 \cdots a_n = b_1 \cdots b_n$ which implies

$$f = q_1 \cdots q_n.$$

This proves existence. Uniqueness follows from the statement that every irreducible is prime (and vice versa). □

Theorem 2.8. *If R is a UFD then so is $R[x]$ and more generally, $R[x_1, x_2, \ldots, x_n]$.*

Proof. This is practically a corollary of the lemma above. □

Note that $\mathbb{Q}[x_1, x_2]$ is not a PID so not a Euclidean ring for example.

3 Vector Spaces: definition and examples

Let F be a field. A *vector space* over F is an abelian group V (in which we write the group law additively) and a *scalar product* which we write as rv for $r \in F$ and $v \in V$ such that for every $r, s \in F$ and $v, w \in V$

1. $r(v + w) = rv + rw$;
2. $(r + s)v = rv + sv$;
3. $r(sv) = (rs)v$;
4. $1v = v$.

3.1 Examples and subspaces

1. Let F^n be the set of all n-tuples $(f_1, \ldots, f_n)$ with $f_i \in F$ for each i. We can regard F^n as a vector space over F.

2. We can regard $F[x]$ as a vector space over F. Also let $F_n[x]$ denote the set of all polynomials $p \in F[x]$ with degree $\leq n$. Then we can regard $F_n[x]$ as a vector space over F.

3. Suppose K is a field and $F \subset K$ is a subfield of K. For example, $\mathbb{Q} \subset \mathbb{R}$ or $\mathbb{R} \subset \mathbb{C}$. In this case, we can regard K as a vector space over F.

4. A *subspace* of a vector space is just a subset that happens to be a vector space when we restrict the scalar product and the additive group law. Equivalently $W \subset V$ is a subspace if W is closed under addition, subtraction and scalar multiplication. For example, we may regard $F_m[x]$ as a subspace of $F[x]$. Also if $F \subset K \subset L$ are fields then we may regard K as a vector subspace of L (where both K and L are considered to be vector spaces over F).

5. Let $F = \mathbb{R}$. Consider $V = \mathbb{R}^{\mathbb{N}} = \{(r_1, r_2, \ldots) : \ r_i \in \mathbb{R}\}$ as a vector space over $\mathbb{R}$. This space has a lot of interesting vector subspaces such as:

   (a) $c_0 = \{(r_1, r_2, \ldots) \in \mathbb{R}^{\mathbb{N}} : \ \lim_i r_i = 0\}$
   (b) $\ell^1 = \{(r_1, r_2, \ldots) \in \mathbb{R}^{\mathbb{N}} : \ \sum_i |r_i| < \infty\}$
   (c) $\ell^2 = \{(r_1, r_2, \ldots) \in \mathbb{R}^{\mathbb{N}} : \ \sum_i |r_i|^2 < \infty\}$
   (d) $\ell^\infty = \{(r_1, r_2, \ldots) \in \mathbb{R}^{\mathbb{N}} : \ \sup_i |r_i| < \infty\}$.

   You should verify that each of these is a vector subspace. It's a bit nontrivial to show that ℓ^2 is closed under addition. You need something called the Cauchy-Schwartz inequality which says that $(\sum_i |r_i + s_i|^2)^{1/2} \leq (\sum_i r_i^2)^{1/2} + (\sum_i s_i^2)^{1/2}$. This comes from an infinite-dimensional generalization of Pythogoras' formula $a^2 + b^2 = c^2$.

4 Homomorphisms, Kernels and Quotients

A map $T : V \to W$ between vector spaces over F is a *homomorphism* if for every $v, w \in V$ and $r, s \in F$,

$$T(rv + sw) = rT(v) + sT(w).$$

We also say that T is F-linear or an F-homomorphism if we need to emphasize the dependence on F.

If T is 1-1 it is said to be an isomorphism or an embedding. Two vector spaces V, W are *isomorphic* if there is a bijective homomorphism between them.

Examples:

- Let $T : \mathbb{C} \to \mathbb{C}$ by $T(a + bi) = a - bi$. Show T is a $\mathbb{Q}$-linear isomomorphism of vector spaces over $\mathbb{Q}$.

- Let $T : \mathbb{Q}[x, y] \to \mathbb{Q}[x]$ be the map $T(p(x, y)) = p(x, 0)$. Show that T is a homomorphism between vector spaces over $\mathbb{Q}$.

What do homomorphism from F^n to F^m "look like"? You should pause and think about this for a minute. You already know the answer when $F = \mathbb{R}$. At least you've seen it before. So think...

Answer: $m \times n$-matrices with values in F. More generally, if we are given vector space V, W over F we let $Hom_F(V, W)$ denote the set of all homomorphisms from V to W. We just denote this by $Hom(V, W)$ if it's safe to leave F implicit. So $Hom(F^n, F^m)$ can be identified with the set of $m \times n$ matrices with values in F.

Note that there is a ring structure to $Hom(V, V)$ (which by the way is often denoted $End(V, V)$ because a homomorphism from V to itself is called an *endomorphism*). The multiplication is given by composition and the addition is well, addition. There is also a scalar multiplication so we can also regard $Hom(V, V)$ as an F-vector space. We won't be studying this very much but it is very interesting.

Definition 3. The *kernel* of a homomorphism $T : V \to W$ is the subspace

$$ker(T) = \{v \in V : \ T(v) = 0\}.$$

You should check that this really is a subspace.

If $V \subset W$ is a subspace then the *quotient space* denoted W/V is the space of cosets of V in W. So $W/V = \{a + V : \ a \in W\}$. There is a canonical homorphism from W onto W/V.

Lemma 4.1. *If $T : V \to W$ is a homomorphism then the image of T is a subspace of W and $V/ker(T)$ is isomorphic to the image of T.*

5 Direct products

If $V_1, \ldots, V_n$ are vector spaces over F then we let

$$V_1 \oplus \cdots \oplus V_n = \{(v_1, \ldots, v_n) : \ v_i \in V_i\}$$

with the obvious vector space structure over F. This is the *direct product* of $V_1, \ldots, V_n$. As a short exercise, you should show that $F^n \oplus F^m$ is isomorphic to F^{n+m} and that F^n is isomorphic to $F \oplus \cdots \oplus F$ (with n summands).

There is a notion of interval direct product: If $V_1, \ldots, V_n$ are *subspaces* of V, and for every $v \in V$ there is a unique $v_1 \in V_1, v_2 \in V_2, \ldots, v_n \in V_n$ such that $v = v_1 + \cdots + v_n$ then we say V is the *internal direct product* of $V_1, \ldots, V_n$.

Theorem 5.1. *If V is the internal direct product of subspaces $V_1, \ldots, V_n$ then V is isomorphic to the direct product $V_1 \oplus \cdots \oplus V_n$.*

(The proof is an easy exercise).

6 Bases, linear independence, dimension

Definition 4. Let V be a vector space over a field F. If $v_1, \ldots, v_n \in V$ and $r_1, \ldots, r_n \in F$ then

$$r_1 v_1 + \cdots + r_n v_n \in V$$

is a *linear combination* over F of the elements $v_1, \ldots, v_n$. We also call this an F-linear combination of $v_1, \ldots, v_n$. The set of all F-linear combinations of $v_1, \ldots, v_n$ is called the *span* of $v_1, \ldots, v_n$. It is a subspace of V denoted $L(v_1, \ldots, v_n)$. If it is all of V then we say that $v_1, \ldots, v_n$ *spans* V. If for every element $v \in L(v_1, \ldots, v_n)$ there is a unique set of scalars $r_1, \ldots, r_n$ such that $v = r_1 v_1 + \cdots r_n v_n$ then we say that $\{v_1, \ldots, v_n\}$ is linearly independent (over F). Otherwise it is *linearly dependent* (over F). If the set $\{v_1, \ldots, v_n\}$ spans V and is linearly independent over F then we say it is a *basis* for V over F.

Lemma 6.1. *If $S \subset V$ is a finite set which spans V then S contains a basis for V.*

Proof. By an inductive argument there exist elements $s_1, \ldots, s_k \in S$ such that $0 \neq L(s_1)$ and $L(s_1, \ldots, s_i) \neq L(s_1, \ldots, s_{i+1})$ for all $1 \leq i < k$ and k is maximal with this property. In particular this means that if t is any element of S then $L(s_1, \ldots, s_k) = L(s_1, \ldots, s_k, t)$. In particular, t is in the span of $\{s_1, \ldots, s_k\}$ so it is an F-linear combination of $s_1, \ldots, s_k$. Since this is true for all $t \in S$, we must have that $L(S) = L(s_1, \ldots, s_k) = V$. It is easy to check that $\{s_1, \ldots, s_k\}$ is linearly independent over F so it is a basis. □

Remark 1. The lemma above is still true when S is infinite but then you need transfinite induction (e.g. Zorn's lemma) to prove it.

Definition 5. We say that V is finite dimensional if there is a finite basis for V.

Lemma 6.2. *Let V be finite-dimensional. If $S \subset V$ is linearly independent then there exists a basis B for V such that $S \subset B$.*

Proof. Let C be a finite basis for V. There exists a maximal set $C' \subset C$ with the property that $S \cup C'$ is linearly independent. Because any $c \in C \setminus C'$ has the property that $C' \cup S \cup \{c\}$ is linearly dependent it follows that $span(S \cup C') = span(S \cup C) = V$. So $S \cup C'$ is a basis for V. □

Lemma 6.3. *Let V be a vector space over F with finite bases S, T. Then S and T have the same number of elements.*

Proof. Let $s \in S$. It follows from the previous lemma (or rather its proof) that there is a subset $T' \subset T$ such that $\{s\} \cup T'$ is a basis for V. We can write s as an F-linear combination in T in a unique way. From this we see that $|T'| = |T| - 1$. (Because $\{s\} \cup T'$ is a basis, any element of T can be expressed in a unique way as an F-linear combination of elements of $\{s\} \cup T'$. We can also express s as a linear combination of elements in T in a unique way. So if $t_1, t_2 \in T \setminus T'$ then

$$t_1 = r_1 s + \sum_{t'_i \in T'} \alpha_i t'_i, \quad t_2 = r_2 s + \sum_{t'_i \in T'} \beta_i t'_i$$

$$s = \sum_{t_i \in T_i} c_i t_i$$

So

$$t_1 = r_1(\sum c_i t_i) + \sum_{t'_i \in T'} \alpha_i t'_i$$

implies that the coefficient $c_2 = 0$ (by uniqueness). Similarly, $c_1 = 0$. But this means that t_1, t_2 can be expressed as combinations of T' which contradicts that T is a basis.)

Now if we list out the elements of S as $S = \{s_1, \ldots, s_n\}$ for some n then we obtain basis $\{s_1, \ldots, s_i\} \cup T_i$ for some $T_i \subset T$ and by induction $|T_i| = |T| - i$. In particular, $S \cup T_n$ is a basis with $|S \cup T_n| = |T|$. But we have to have $T_n = \emptyset$ because S is already a basis. So we have to have $|S| = |T|$ as required. □

The lemma above allows us to define the F-dimension of a vector space as the cardinality of any basis. Note that the dimension depends on the field F. For example, the $\mathbb{R}$-dimension of $\mathbb{C}$ is .... (you supply the answer). But the $\mathbb{Q}$-dimension of $\mathbb{C}$ is ....

Lemma 6.4. *If V, W are vector spaces over F and the F-dimensions of V and W are finite and equal then V is isomorphic to W (as F-vector spaces).*

Proof. Let B be a basis for V, C a basis for W and let $T : B \to C$ be a bijection. We extend T by linearity. Show that this defines an isomorphism. □

Lemma 6.5. *If $T : V \to W$ is a homomorphism and V is finite-dimensional then*

$$dim_F(ker(T)) + dim_F(Image(T)) = dim_F(V).$$

Proof. The idea of the proof is that we can construct a basis for V from a basis for $ker(T)$ and a basis for $Im(T)$. □