1.5 06/19/24 - Irreducibility I and Unique Factorization I

Last time, we showed that if $C \subset \mathbb{A}^2_k$ is an algebraic curve over an algebraically closed field k, then C is nonempty (and, in fact, infinite). Let's record this fact here, since I left some of it to you as an exercise.

Lemma 1.5.1. If k is an algebraically closed field, then any curve $C \subset \mathbb{A}^2_k$ is infinite.

Henceforth, we will always assume that our base field k is algebraically closed; this will simplify life for us tremendously. If time permits, we will return to non algebraically closed fields towards the end of the course.

1.5.1 Irreducibility I

Today I want to spend some more time relating the algebra of $k[x, y]$ to the geometry of curves in $\mathbb{A}^2_k$. Consider the following parallel definitions:

Definition 1.5.2. Let R be a ring.

(a) An element $f \in R$ is said to be irreducible if it is not zero, not a unit, and if $f = gh$ for some $g, h \in R$, then either g or h is a unit.
(b) An element $f \in R$ is said to be a prime if it is not zero, not a unit, and if $f|gh$ for some $g, h \in R$, then either $f|g$ or $f|h$.

Definition 1.5.3. A curve $C \subset \mathbb{A}^2_k$ is said to be irreducible if whenever $C = D \cup E$ for curves $D, E \subset \mathbb{A}^2_k$, then either $D = C$ or $E = C$.

Remark 1.5.4. The condition in Definition 1.5.2(b) says that a nonzero $f \in R$ is prime iff the principal ideal $(f) \subset R$ generated by f is a prime ideal. If R is an integral domain, then every prime is irreducible, but the converse need not hold in general–see Exercise 2.3.2. The converse does, however, hold if R is a UFD; see Proposition 1.5.8.

What is the relationship between the irreducibility of a polynomial and that of the curve defined by it? In light of Proposition 1.1.7, one could reasonably make

Conjecture 1.5.5. Give a nonconstant polynomial $f \in k[x, y]$, the algebraic curve C_f defined by f is irreducibe iff f is.

However, a moment's reflection shows that this cannot be correct as stated. For instance, if $f(x, y) = x^2$, then f is not irreducible, but the algebraic curve C_f is a line, which is irreducible thanks to Exercise 2.1.7 (how?). One correct salvage of this statement would be

Theorem 1.5.6. If an $f \in k[x, y]$ is irreducible, then C_f is irreducible, and conversely if $C \subset \mathbb{A}^2_k$ is an irreducible curve, then there is an irreducible $f \in k[x, y]$ such that $C = C_f$.

Our next order of business is to develop tools to prove Theorem 1.5.6.

1.5.2 Unique Factorization I

The first fact we would need is that $k[x, y]$ is UFD. Let's recall the definition of such a ring.

Definition 1.5.7. A ring is said to be a unique factorization domain, abbreviated UFD, if R is a domain[a], if every nonzero nonunit in it is a product of finitely many irreducible elements, and the decomposition into irreducible factors is unique up to order and multiplication by units. In other words, a domain R is a UFD if given any nonzero nonunit $f \in R$, there is an integer $n \geq 1$ and irreducible elements $f_1, \ldots, f_n \in R$ such that

$$f = f_1 f_2 \cdots f_n$$

and if there is some other integer $m \geq 1$ and irreducible elements $g_1, \ldots, g_m \in R$ such that

$$f = f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m,$$

then we must have $n = m$, a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ and units $c_1, \ldots, c_n \in R^\times$ such that for all i with $1 \leq i \leq n$ we have $c_i g_i = f_{\sigma(i)}$.

[a] This means the same thing as "integral domain".

A field is vacuously a UFD–there *are* no nonzero nonunits. Here's one way to identify UFD's.

Proposition 1.5.8. Let R be a domain. Then the following are equivalent:

(a) R is a UFD.
(b) Every nonzero nonunit in R is a product of finitely many irreducible elements and each irreducible element is prime.
(c) Every nonzero nonunit in R is a product of finitely many prime elements.

Proof.

(a) $\Rightarrow$ (b) We only need to show that every irreducible in a UFD is prime; I leave this to the reader.

(b) $\Rightarrow$ (c) Clear.

(c) $\Rightarrow$ (a) Since primes are irreducible, all that remains to be shown is uniqueness of factorization. For this, we first show that if (c) holds, then every irreducible element is prime: indeed, if $f \in R$ is irreducible and we write $f = p_1 \cdots p_n$ for some integer $n \geq 1$ and primes $p_1, \ldots, p_n$, then irreducibility of f tells us (how?) that $n = 1$ and $f = p_1$ is prime. We show uniqueness of the irreducible decomposition of a nonzero nonunit $f \in R$ by inducting on the minimal number $n \geq 1$ of irreducible factors in such a decomposition. For the base case $n = 1$, our $f = f_1$ itself is irreducible, so if $f = g_1 \cdots g_m$ for some $m \geq 1$ and irreducibles $g_j \in R$, then irreducibility of f tells us (how?) that $m = 1$ and $f = g_1$. Inductively, if we have for some $m \geq n \geq 2$ that

$$f = f_1 \cdots f_n = g_1 \cdots g_m,$$

then primality of g_1 tells us that $g_1 \mid f_j$ for some j with $1 \leq j \leq n$, so let $c_1 \in R$ be such that $c_1 g_1 = f_j$. Now f_j is irreducible and g_1 is not a unit, so c_1 must be a unit. Therefore, cancelling f_1 from both sides, we are left with

$$f_1 \cdots f_{j-1} f_{j+1} \cdots f_n = (c_1^{-1} g_2) g_3 \cdots g_m,$$

so we are done by induction (how?).

■

The one technique we have seen at Ross so far of showing that a domain is a UFD is to work with Euclidean functions. Let's define those now.

Definition 1.5.9.

(a) Let R be a domain. A Euclidean function on R is a map $d : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $A, B \in R$ with $B \neq 0$, there are $q, r \in R$ such that

$$A = Bq + r$$

and either $r = 0$ or $d(r) < d(B)$.

(b) A domain R is said to be a Euclidean domain if it admits a Euclidean function.

Here are a few key examples.

Example 1.5.10.

(a) For $R = K$ a field, the function $d \equiv 1$ is Euclidean.
(b) For $R = \mathbb{Z}$, the function $d(n) = |n|$ is Euclidean.
(c) For $R = \mathbb{Z}[i]$ or $R = \mathbb{Z}[\omega]$, the norm function $d(\alpha) = \mathrm{N}(\alpha)$ is Euclidean.
(d) For $R = K[t]$, the polynomial ring over the field K, the function $d(f) = \deg f$ is Euclidean.
(e) For $R = K[\![t]\!]$, the $d(f) = \mathrm{ord}_t f$ taking a power series to the highest power of t dividing it is Euclidean.

The key reason we like Euclidean domains is

Theorem 1.5.11. Every Euclidean domain is a UFD.

Proof Sketch. The key idea is that Euclidean functions allow us to perform the Euclidean algoritheorem to produce the greatest common divisor of any two elements, although I do want to warn you that the proof at this level of generality needs some work. See [2] for a direct proof, or any algebra textbook. ■

The result that we really need, however, is that the ring $R = k[x, y]$ is a UFD. This cannot be done using Theorem 1.5.11–indeed, the ring $k[x, y]$ is not a Euclidean domain.[12] How do we proceed then?

We will prove

Theorem 1.5.12. If R is a UFD, then so is the polynomial ring $R[t]$.

Remark 1.5.13. In fact, one can check that if R is any ring such that $R[t]$ is a UFD, then so is R. (Prove this!) This makes the statement in Theorem 1.5.12 an "if-and-only-if" statement.

The way we will we use Theorem 1.5.12 is via

Corollary 1.5.14. If R is a UFD, then so is the polynomial ring $R[t_1, \ldots, t_n]$ for each $n \geq 1$. In particular, for any field k, the ring $k[x, y]$ is a UFD.

[12] This is because Euclidean domains are principal ideal domains, while $k[x, y]$ is not one. If you don't know what this means, you can ignore this comment. If you do know what this means, there are also examples of principal ideal domains which are not Euclidean, but such rings are harder to come by. The simplest examples I know of are $R = \mathcal{O}_{\mathbb{Q}[\sqrt{-19}]}$ and $R = \mathbb{R}[x, y]/(x^2 + y^2 + 1)$, but proving these claims needs some work.

To prove Theorem 1.5.12, we need some preparation. In what follows, we will fix a UFD R and let $K = \operatorname{Frac} R$ be its fraction field, so that $K = \{p/q : p, q \in R, q \neq 0\}$. Also, for any $f \in R[t]$ and $n \geq 0$, we will denote the coefficient of t^n by $[t^n]f$. The first order of business is to show that $R[t]$ is a domain.

Lemma 1.5.15.

(a) If R is a domain, then so is $R[t]$.
(b) If $p \in R$ is prime, then p is also prime in $R[t]$.

Proof.

(a) Write $0 \neq f, g \in R[t]$ as $f = \sum_{i=0}^{n} a_{n-i}t^i$ and $g = \sum_{j=0}^{m} b_{m-j}t^j$ for some $m, n \geq 0$, with $a_i, b_j \in R$ and $a_0 \neq 0$ and $b_0 \neq 0$. Since R is a domain, $[t^{m+n}]fg = a_0b_0 \neq 0$, so $fg \neq 0$.
(b) We can either reduce to (a) by noticing that $R[t]/(p) \cong (R/p)[t]$ (how?), or argue directly as before: if $f \in R[t]$ is such that $p \nmid f$ and we write $f = \sum_{i=0}^{n} a_{n-i}t^i$ for some $n \geq 0$ and $a_i \in R$ with $a_0 \neq 0$, then there is some i with $0 \leq i \leq n$ and $p \nmid a_i$; let i_0 be the smallest such i. Similarly, if $p \nmid g$, then write $g = \sum_{j=0}^{m} b_{m-j}t^j$ as in (a) and pick the smallest j_0 with $0 \leq j_0 \leq m$ such that $p \nmid b_{j_0}$. Then, $p \nmid [t^{(m-i_0)+(n-j_0)}]fg$ (check!) so that $p \nmid fg$.

■

Definition 1.5.16. A polynomial $f \in R[t]$ is said to be primitive if the following equivalent conditions hold:

(a) If $\alpha \in R$ is such that $\alpha \mid f$, then α is a unit.
(b) There is no prime $p \in R$ such that $p \mid f$, i.e. $p \mid [t^i]f$ for all $i \geq 0$.
(c) The greatest common divisor of all coefficients of f is (1).

Note that 0 is not primitive. Any $f \in K[t]$ can be written as $f = \operatorname{cont}(f) \cdot \tilde{f}$ for some $\operatorname{cont}(f) \in K$ and primitive $\tilde{f} \in R[t]$. If $f \neq 0$, then $\operatorname{cont}(f)$ and $\tilde{f}$ are uniquely determined up to units in R; then $\operatorname{cont}(f)$ is called the content of f, and $\tilde{f}$ is called the primitive part of f, defined uniquely only up to units in R.[13] Here are some basic properties that we will need:

Lemma 1.5.17. If $0 \neq f \in K[t]$, then

(a) $\deg \tilde{f} = \deg f$,
(b) $\operatorname{cont}(f) = f$ iff f is constant,
(c) $f \in R[t]$ iff $\operatorname{cont}(f) \in R$,
(d) if (c) holds, then f is primitive iff $\operatorname{cont}(f)$ is a unit in R, and
(e) $\tilde{\tilde{f}} = \tilde{f}$.

Proof. Left to the reader. ■

The key result that allows us to relate $R[t]$ and $K[t]$ is

[13] One way to make this precise is to say that the fractional ideal $(\operatorname{cont} f)$ of R and the (integral) ideal $(\tilde{f})$ of $R[t]$ are uniquely determined. We will not need these notions. When we assert an equality involving $\operatorname{cont}(f)$ or $\tilde{f}$, that equality will always be assumed to hold up to units.

Lemma 1.5.18 (Gauss's Lemma).

(a) If $f, g \in R[t]$ are primitive, then so is fg. In general, if we have nonzero $f, g \in K[t]$, then $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$ and $\widetilde{fg} = \tilde{f}\tilde{g}$ (up to units). The same holds for any number $f_1, \ldots, f_n$ of elements with $n \geq 1$.
(b) If $f, g \in R[t]$ are nonzero such that $f \mid g$ in $K[t]$ and f is primitive, then $f \mid g$ in $R[t]$.
(c) If $f \in R[t]$ is primitive and prime in $K[t]$, then f is prime in $R[t]$.

Proof.

(a) The general case follows by induction, so we do the case $n = 2$. If $f, g \in R[t]$ are primitive and if a prime $p \in R$ were to divide fg, then it would divide either f or g by Lemma 1.5.15(b). In general, given nonzero $f, g \in K[t]$, we have $fg = \operatorname{cont}(f)\operatorname{cont}(g) \cdot \tilde{f}\tilde{g}$, and $\tilde{f}\tilde{g}$ is primitive by the first part, so by the uniqueness of this deomposition we must have $\widetilde{fg} = \tilde{f} \cdot \tilde{g}$, and hence that $\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.
(b) If $g = fq$ for some nonzero $q \in K[t]$, then $\operatorname{cont}(g) = \operatorname{cont}(f) \cdot \operatorname{cont}(q)$. Since $f, g \in R[t]$, Lemma 1.5.17(c) tells us that $\operatorname{cont}(f), \operatorname{cont}(g) \in R$, and since f is primitive, Lemma 1.5.17(d) tells us that $\operatorname{cont}(f)$ is a unit, so that $\operatorname{cont}(q) = \operatorname{cont}(g)\operatorname{cont}(f)^{-1} \in R$, and hence by Lemma 1.5.17(c) again we conclude that $q \in R[t]$.
(c) Suppose $f \in R[t]$ is primitive and prime in $K[t]$ (and hence nonzero), and suppose $f | gh$ for some $g, h \in R[t]$. Then $f \mid gh$ also in $K[t]$, and so by primality either $f | g$ or $f | h$ in $K[t]$, and hence also in $R[t]$ by (b), showing that f is prime in $R[t]$.

■

In Lemma 1.5.18(b), we certainly need f to be primitive; a simple counterexample otherwise is given by taking $R = \mathbb{Z}$ and $f(t) = 2t$ and $g(t) = t$. We are now ready to prove Theorem 1.5.12.

Proof of Theorem 1.5.12. Suppose R is a UFD and $K = \operatorname{Frac} R$. By Proposition 1.5.8(c), it suffices to show that every nonzero nonunit $f \in R[t]$ is a product of finitely many primes. Since $f = \operatorname{cont}(f) \cdot \tilde{f}$, it suffices to show that each of $\operatorname{cont}(f)$ and $\tilde{f}$ is a product of finitely many primes in $R[t]$.[14]

Since $0 \neq \operatorname{cont}(f) \in R$ and R is a UFD, either $\operatorname{cont}(f)$ is a unit in R (and hence in $R[t]$), or it is a product of one or more primes in R. Since primes in R are primes in $R[t]$ by Lemma 1.5.15(b), it follows that $\operatorname{cont}(f)$ is a product of finitely many primes in $R[t]$.

Now consider the primitive part $0 \neq \tilde{f} \in R[t]$. Since $K[t]$ is a UFD, it follows that either $\tilde{f}$ is a unit in $K[t]$ or it is the product of one or more primes in $K[t]$. In the former case, $\tilde{f}$ is constant[15] and so since it is primitive, it must be a unit in R (by Lemma 1.5.17(b) and (d)). In the latter case, $\tilde{f}$ is the product of one or more primes in $K[t]$, say $\tilde{f} = f_1 \cdots f_n$ for some $n \geq 1$, where for $1 \leq j \leq n$, each $f_j \in K[t]$ is prime. Then using Lemma 1.5.17(e) and Lemma 1.5.18(a), we find that

$$\tilde{f} = \widetilde{\tilde{f}} = \tilde{f}_1 \cdots \tilde{f}_n.$$

For each j, the element $\tilde{f}_j \in R[t]$ is primitive and prime in $K[t]$ (since it is a nonzero constant, i.e. unit, times the prime f_j in $K[t]$), and so by Lemma 1.5.18(c) is a prime in $R[t]$. Therefore, we have exhibited $\tilde{f}$ as a product of one or more primes in $R[t]$, finishing the proof. ■

[14] Note that finitely many also includes zero many–i.e. it is okay for $\operatorname{cont}(f)$ or $\tilde{f}$ to be a unit in $R[t]$, but if both are units in $R[t]$, then so is $f = \operatorname{cont}(f) \cdot \tilde{f}$.

[15] This is because the only units in $K[t]$ are constants, i.e. elements of $K^\times = K \smallsetminus \{0\}$. If you haven't seen this before, prove it!