What is commutative algebra?

In school and intro univ. algebra you studied _division with remainder_ for integers and polynomials in k[x].

Integers: given a,b positive integers, you can write
   a = b*q + r with 0 <= r < b.
If you have a cakes to give to b kids, hand them out equally b at a time until the remainder r < b is not enough to go around.

Polynomials: given A, B in k[x]
  A = an x^n + a_{n-1}x^{n-1} + .. a0
  B = bm x^m + .. b0
with deg A = n, deg B = m (deg means top term <> 0). If m <= n we can subtract a multiple of g to cancel the top term in f:
  A - an/bm*x^{n-m}*B of deg <= n-1.
Just continue decreasing deg A until deg (A - (mult. q*B)) < m.
(We will see later that removing the leading term is also an important idea in constructing a Groebner basis.)

In either case we have a notion of size of A, and can successively reduce it by subtraction to < size B, (and the logic has an initial case size B = 0).

The point I want to make is that the objects we are talking about are quite different: integers versus polynomial functions or abstract polynomials. Nevertheless, the methods of argument are exactly the same.

Please think through the argument used to show:

ZZ and k[x] have division with remainder, so are PID: every ideal I is generated by a single element, I = (f)). And

PID is a UFD: every element factorises as a product of a unit times a product of prime powers, uniquely up to units and order of the factors. This gives the usual properties of GCD and LCM, including the important a*f + b*g = h property of h = GCD(f,g).

==
What is commutative algebra?

The 1882 paper [DW] extended this analogy in elementary algebra to a theory that encompasses both the ring of integers of a number field and the ring of functions on an algebraic curve. Their paper is a landmark in the development of modern algebra, and marks the starting point of commutative algebra.

[DW] Richard Dedekind and Heinrich Weber, Theorie der algebraischen Funktionen einer Veränderlichen, J. reine angew. Math. 92 (1882), 181--290

I explain this briefly (don't worry about the details -- I will return to the full arguments later).

==
Ring of integers of an algebraic number field

An _algebraic number field_ is a finite extension field QQ in K. Corresponding to the ring of integers ZZ in QQ, the field K also has a subring O_K of integers, the subset of K of integral elements (details later). In any fairly complicated case, the division with remainder that we used for ZZ does not work for O_K, and it is _not_ a UFD.

==
Integral closure of an algebraic function field

You know the polynomial ring k[x] over a field k (say k = CC to be definite). Its field of fractions k(x) consists of rational functions f(x)/g(x) with f,g polynomials and g <> 0. An _algebraic function field_ in one variable is a finite extension field k(x) in K (where x is transcendental).

Corresponding to the polynomial ring k[t] in k(t), the same definition as the number field case gives the integral closure A of k[x] in K: A is the subset of elements of K that are _integral_ over k[x] (satisfy a monic equation with coefficients in k[x] -- no denominators allowed, and leading coefficient 1). This integral closure A = k[C] is the coordinate ring of a nonsingular affine algebraic curve C over k. (I am not saying that this is obvious.) In any fairly complicated case, this A does not have division with remainder, and is _not_ a UFD.

==
Dedekind and Weber's synthesis

The preceding paragraphs set up the ring of integers O_K of a number field K, and the coordinate ring k[C] of a nonsingular affine curve C. These objects are major protagonists of algebraic number theory and algebraic geometry, and are clearly very different in nature. However, Dedekind and Weber [DW] say that these two rings can be studied using the same algebraic apparatus. As I said, they are usually not UFDs.

The good news: if A is a ring of either type (a Dedekind domain), the ideals of A have _unique factorisation into prime ideals_.

The key method of argument is _localisation_ (partial ring of fractions). If P is a prime ideal of A, the localisation of A at P is A_P = S^-1A where S = multiplicative set S = A - P.

(I will go through this in detail later.) In arithmetic, A_P in K is the algebraic numbers that have an expression f/g with g notin P. For a point P of and algebraic curve C, A_P consists of the rational functions in k(C) that have an expression f/g with denominator g not vanishing at P in C.

For either kind of ring A_P is a discrete valuation ring (DVR). Although when the ring A is not a UFD, its localisation A_P is the simplest possible UFD: it has a single prime element z (up to units), and every nonzero element h in K has the factorisation

  h = z^n*(unit), where n = v_P(h) is the valuation of h at P.

Valuations then determine everything about A in K and the ideals of A: an element h in K is in A if and only if it has valuation >= 0 at every P. Moroever, every ideal I in A also has a valuation at P (namely, min v_P(i) taken over i in I). For any given nonzero ideal I of A, there are just finitely many primes P such that v_P(I) > 0, and I equals the product of P^v_P(I).

==
Modern abstract algebra

Notice the breakthrough aspect of Dedekind and Weber: modern algebra has axioms and abstract arguments, and you often work with objects in a symbolic way. In this case, without reference to what the elements of the ring actually are.