.

UGC Refresher Course

University of Mysore

November 2003

Lectures on commutative rings by

B.Sury
Indian Statistical Institute
Bangalore.

Introduction

We discuss the basic facts, notions and results of commutative ring theory. We recall them in a form which will be suitable for discussing Galois theory and algebraic number theory. At the end, we list ten problems.

§ 1 Commutative rings - Basic notions

The rings we consider for our purposes here are all commutative and have a multiplicative unity.

• 1.1 *Integral domains, nilpotent elements and units*

A non-zero element $a \in A$ of a ring A is a *zero-divisor* if there exists $b \neq 0$ such that $ab = 0$. A ring without zero divisors is called an *integral domain* or simply a domain.
The ring $\mathbf{Z}/n\mathbf{Z}$ is a domain if and only if $n = 0$ or n is a prime.

It is an easy exercise to show that the rings $C([0,1],\mathbf{R}), C^{\infty}([0,1],\mathbf{R})$ of continuous and smooth real-valued functions defined on the interval $[0,1]$ are not integral domains. The subring of real analytic functions is a domain. So, is the ring of holomorphic functions on a complex region since the zeroes of holomorphic functions are isolated.
For polynomials f, g in a single variable with coefficients in a domain A, the degree of fg is the sum of the degrees of f and g. Thus, we have :
A is an integral domain if, and only if, $A[X]$ is.
An element a in a ring A is said to be *nilpotent* if $a^n = 0$ for some $n \geq 1$.
An element $u \in A$ is said to be a *unit* if there exists $v \in A$ such that $uv = 1$.
The subset A^* of all units in A is a group under multiplication.
Recall that an additive subgroup I of a ring A is said to be an *ideal* if $ab \in I$ for all $a \in A, b \in I$.

The set of all nilpotent elements forms an ideal Nil(A) called the nil radical of A.
For, if $a^m = 0 = b^n$, then $(a \pm b)^{m+n} = 0$.
If $u \in A^*, a \in Nil(A)$, then $u - a \in A^*$.
For, if $uv = 1$ and $a^n = 0$, then $(u-a)^{-1} = (u(1-va))^{-1} = v(1 + va + \cdots + v^{n-1}a^{n-1})$.
Later, we shall see that Nil (A) is the intersection of all the prime ideals of

A.
Clearly, $C([0,1], \mathbf{R})$ has no non-zero nilpotents.

If $f = a_0 + a_1X + \cdots + a_nX^n$ is in $A[X]$ for some A, then f is nilpotent if, and only if, all $a_i (i \geq 0)$ are nilpotent.
This can be proved by induction on n as follows. It is clearly true when $n = 0$. Now, if $n > 0$, and $f^r = 0$, then $a_n^r = 0$, that is, a_n is nilpotent. Thus, $f - a_nX^n$ is nilpotent. Hence all $a_i, 0 \leq i < n$ are nilpotent.
Note that in any ring R and for $u \in R^*$ and x nilpotent, the elements $u - xy$ are units for all y; indeed $(u - xy)^{-1} = u^{-1}(1 - u^{-1}xy)^{-1} = u^{-1} \sum_{i=0}^{k} u^{-i}x^iy^i$ where $x^{k+1} = 0$.

Using the above fact, we can show :
$f = \sum_{i=0}^{n} a_iX^i \in A[X]^*$ *if, and only if, $a_0 \in A^*$ and $a_i (i \geq 1)$ are nilpotent.*
Indeed, the 'if' part is clear by the above comment. For the 'only if' part, assume that $g = \sum_{i=0}^{m} b_iX^i$ is the inverse of f. If $n = 0$, then $a_0 \in A^*$. Let $n > 0$ and suppose the result holds for units in $A[X]$ of degrees less than n. Now, clearly $a_0 \in A^*$ and, inductively, $a_n^{i+1}b_{m-i} = 0$; so $a_n^{m+1} = 0$ i.e., a_n is nilpotent. Thus, $f - a_nX^n$ is a unit. By the induction hypothesis, all the a_i's with $i > 0$ are nilpotent.

$f = \sum_{i \geq 0} a_iX^i \in A[[X]]$ *is a unit in it if, and only if, a_0 is a unit.*
This is obvious.

Let $\alpha \in \mathbf{C}$ be an 'algebraic integer' i.e., α satisfies some monic integral polynomial (e.g. $\alpha = \sqrt{2}$). Then, $A = \{$ all finite sums $\sum a_i\alpha^i; a_i \in \mathbf{Z}\}$ is an integral domain which is finitely generated as an abelian group. It is a deep theorem of Dirichlet that A^* is a finitely generated abelian group.

• 1.2 *Prime ideals, maximal ideals*

Clearly, an ideal I is proper (i.e. not the whole of A) if, and only if, $1 \notin I$.
A proper ideal M is said to be *maximal* if it is not strictly contained in any other proper ideal. It follows by using Zorn's lemma that :
Any proper ideal I is contained in a maximal ideal.
For, let F be the family of all proper ideals containing I. This is a non-empty set since $I \in F$. Let C be any chain of proper ideals containing I; then the union of all the ideals in C is a proper ideal since 1 cannot belong to it. Hence, by Zorn's lemma, F has a maximal element. Such an element M is a maximal ideal since any proper ideal properly containing M would be in F

and would contradict the maximality of M in F.

A proper ideal P is said to be a *prime* ideal if $ab \in P$ implies either $a \in P$ or $b \in P$.
Any maximal ideal is a prime ideal. In any domain, $\{0\}$ *is a prime ideal.*

Notice that, in $\mathbf{Z}$, the zero ideal is prime but not maximal; every other prime ideal is maximal and is given as multiples of some prime number. The rings studied in number theory are integral domains in which all ideals are finitely generated and have the property that all nonzero prime ideals are maximal. They are known as Dedekind domains. In fact, ideals in such domains of number theory are not singly generated in general, and this is the fundamental cause for problems like Fermat's last theorem being very hard.

I is a prime ideal of a ring A if, and only if, the quotient ring A/I is a domain. I is maximal if, and only if, A/I is a field.

In $A[X]$, where A is an integral domain, the polynomials with constant term 0 form a prime ideal which is maximal if, and only if, A is a field.
This statement follows since $A[X]/(X) \cong A$.

In $A = C([0,1], \mathbf{R})$, for each point $x \in [0,1]$, one has a maximal ideal $M_x = \{f \in A : f(x) = 0\}$. Moreover, any maximal ideal is of this form for some x.
This is a simple consequence of the compactness of $[0,1]$ as follows. Before starting with the proof, observe that any finite set $f_1, \cdots, f_r$ of elements in $C[0,1]$ must have a common zero unless they generate the unit ideal (if they have no common zero, then $1 = \sum_i g_i f_i$ with $g_i = f_i / \sum_i f_i^2$).
Let M be a maximal ideal and suppose that no point in $[0,1]$ is a common zero for all functions in M. To each $x \in [0,1]$, let $g_x \in M$ with $g_x(x) \neq 0$. As g_x is continuous, there exists a neighbourhood V_x of x such that $g_x(y) \neq 0$ for all $y \in V_x$. Since $[0,1] = \bigcup_x V_x$, one may write (by compactness) $[0,1] = \cup_{i=1}^{r} V_{x_i}$ for some $x_i \in [0,1]$. By the observation made in the beginning, g_{x_i} have a common zero; however, this cannot belong to any V_{x_i}, a contradiction. Therefore, $M \subseteq M_x$ for some x. As both are maximal, they are equal.

In fact, the analogue of the last statement is false for the ring $C((0,1), \mathbf{R})$. For, one may consider the ideal generated by all functions which vanish outside some compact set. A maximal ideal containing such an ideal cannot be of the above form.

In $C[0,1]$, there are prime ideals which are not maximal.
For example, let S denote the subset of A consisting of all monic polynomials. Then, by Zorn's lemma, one can see that there is an ideal P of A which does not intersect S and is maximal with respect to this property. It is trivial to see that P must be prime (see the next section on localisation for a generalisation).
However, if it were maximal, then it would be M_a for some $a \in [0,1]$. This is impossible, for, then the function $f(x) = x - a$ would be in S as well as in P. Thus P is not maximal.

One has certain special properties for prime ideals in any commutative ring. For instance :
If a prime ideal P contains $I \cap J$, then it must contain one of I and J.
For, if $a \in I, b \in J$ and $a, b \notin P$, then $ab \in I \cap J \subseteq P$ which implies either a or b must be in P, a contradiction.
Under any ring homomorphism, the inverse image of a prime ideal is again a prime ideal.
This is not true for maximal ideals; for instance consider the inverse image of the maximal ideal $\{0\}$ of $\mathbf{Q}$ under the inclusion of $\mathbf{Z}$.

• 1.3 **Chinese remainder theorem for rings**

This is the following theorem and has several interesting applications. The classical Chinese remainder theorem for which solves simultaneous congruences is obtained by appllying the surjectivity of the map below applied to the ring of integers.

Let $I_1, \cdots, I_n$ be coprime ideals (i.e., $I_1 + \cdots + I_n = A$). Then, $A/(\cap_i I_i) \cong \oplus_i A/I_i$.
By induction on n, this easily reduces to $n = 2$. Now, $1 = x_1 + x_2$ for some $x_i \in I_i$. The homomorphism $\pi\ A \to A/I_1 \oplus A/I_2$ which is the combination of the two natural homomorphisms has clearly the kernel $I_1 \cap I_2$. The nontrivial part is the surjectivity. For this, take any $(y_1 + I_1, y_2 + I_2) \in A/I_1 \oplus A/I_2$. This is clearly $\pi(x_1 y_2 + x_2 y_1)$. This shows surjectivity.

Here is one nice application of the Chinese remainder theorem :
The number of ring homomorphisms from $\mathbf{Z}/m$ to $\mathbf{Z}/n$ is $2^{\omega(n) - \omega(\frac{n}{(m,n)})}$. Here $\omega(n)$ stands for the number of prime divisors of n.
Proof.

Let $\theta : \mathbf{Z}/m \to \mathbf{Z}/n$ be one such. Write $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then, $\mathbf{Z}/n \cong \mathbf{Z}/p_1^{\alpha_1} \times \cdots \times \mathbf{Z}/p_r^{\alpha_r}$ as rings. Write $\theta(1) = (a_1, \cdots, a_r)$. Now, $\theta(1) = \theta(1^2)$ gives that $a_i = a_i^2$ in $\mathbf{Z}/p_i^{\alpha_i}$ for each i. As $(a_i, a_i - 1) = 1$, either $a_i \equiv 0$ or $\equiv 1$ mod $p_i^{\alpha_i}$. Also, $0 = m\theta(1) = \theta(m) = (ma_1, \cdots, ma_r)$. Thus, $ma_i \equiv 0$ mod $p_i^{\alpha_i}$ for all $i \leq r$. If, for some i, we have $a_i \not\equiv 0$ mod $p_i^{\alpha_i}$, then $a_i \equiv 1, ma_i \equiv 0$ gives that $p_i^{\alpha_i} | m \quad \cdots (\spadesuit)$.
Write $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \cdots p_r^{\alpha_r}$ where $p_i^{\alpha_i} | m$ for all $i \leq s$ and $p_i^{\alpha_i} \not| m$ for all $i > s$. Therefore, the above observation $(\spadesuit)$ implies that $a_i \equiv 0$ mod $p_i^{\alpha_i}$ for all $i > s$ and $a_i \equiv 0$ or 1 mod $p_i^{\alpha_i}$ for all $i \leq s$.
Hence, the number of ring homomorphisms from $\mathbf{Z}/m$ to $\mathbf{Z}/n$ is 2^s. Clearly, $s = \omega(n) - \omega(\frac{n}{(m,n)})$.

An application of the Chinese remainder theorem to linear algebra arises by considering the ring $K[X]$ for any field K. Before stating it, recall that a matrix $N \in M_n(K)$ is said to be nilpotent if all its eigenvalues are 0. A matrix $S \in M_n(K)$ is said to be semisimple if its minimal polynomial has distinct roots; this means that S is conjugate over the algebraic closure of K to a diagonal matrix. We have:

(Jordan decomposition) Any matrix $A \in M_n(K)$ can be written as $A = S + N$ with S semisimple N nilpotent and both S, N are polynomials in A without constant term.
Note that the expression of a matrix as a sum of a semisimple and a nilpotent matrix which commute with each other must be unique. This is because the only matrix which is both semisimple and nilpotent is the zero matrix. So, if $A = S_0 + N_0$ for another commuting pair, then S_0 and N_0 commute with A and, therefore, with S, N also. Thus, $S + N = S_0 + N_0$ gives $S - S_0 = N_0 - N$ which must be zero.
Proof of existence.
Over $\bar{K}$, the characteristic polynomial $\chi_A(T)$ can be written as $\prod_{i=1}^r (T - \lambda_i)^{n_i}$. In $K[T]$, let us find, by the CRT, an element $\phi(T)$ such that

$$\phi(T) \equiv \lambda_i \ \ mod \ \ (T - \lambda_i)^{n_i},$$

$$\phi(T) \equiv 0 \ \ mod \ \ T.$$

If $V_i = ker(A - \lambda_i)^{n_i}$, we have $\bar{K}^n = \oplus_{i=1}^r V_i$. Thus, the matrix $S := \phi(A)$ acts as the scalar λ_i on V_i. So, S is semisimple. Further, it is a polynomial in A without constant term. If $N := A - S$, then N has only zero as eigenvalues

and it must be nilpotent. Of course, N is also a polynomial in A without constant term. This proves the decomposition asserted.

- 1.4 **Localisation**

Every domain A can be realised as a subring of a field K which is the smallest such in the sense that any ring homomorphism from A to a field L extends to a unique homomorphism from K to L. The field K is called the quotient field of A and can be constructed as follows: on pairs of elements (a, b) with $b \neq 0$, consider the equivalence relation defined as $(a, b) \sim (c, d)$ if, and only if, $ad = bc$. The equivalence classes can naturally be thought of as the fractions a/b and they form the quotient field K.
The quotient field of $A[X]$ is $Q(A)(X)$ for any domain A where $Q(A)$ is the quotient field of A and $Q(A)(X)$ stands for the set of rational functions $\frac{f(X)}{g(X)}$ with coefficients from $Q(A)$.
Thus, the quotient field of an integral domain is obtained by 'inverting' all non-zero elements. More generally, let A be a commutative ring with unity (not necessarily a domain) and $S \subset A$ be a multiplicatively closed subset i.e., $1 \in S$ and S is closed under mutiplication. Then, one can form a new ring by 'inverting the elements of S' as follows. On pairs of elements $(a, s) \in A \times S$, define a relation $(a, s) \sim (b, t)$ if, and only if, $\exists s_0 \in S$ such that $s_0(ta - sb) = 0$. This is an equivalence relation and the set $S^{-1}A$ of equivalence classes naturally has a ring structure. Indeed, think of the class of a pair (a, s) as the 'fraction' $\frac{a}{s}$. The ring $S^{-1}A$ is called the localisation of A at S. There is a natural ring homomorphism from A to $S^{-1}A$ given by $a \mapsto \frac{a}{1}$. This is, in general, not injective but it is so if A is a domain.
A typical example is when S is the complement in A of a prime ideal P. In this case, one usually denotes $S^{-1}A$ by A_P. Notice that when A is a domain, then $\{0\}$ is a prime ideal and the corresponding localisation is just the quotient field.
For a general A (i.e., not necessarily a domain), the prime ideals of $S^{-1}A$ are in bijective correspondence with the set of prime ideals of A which do not intersect S. In particular, if $S = A \setminus P$ for some prime ideal P, then A_P is a local ring i.e., it has only one maximal ideal $S^{-1}P$.
In algebraic geometry as well as in algebraic number theory, many local rings arise naturally. For instance, consider the ring A of "germs" of continuous functions at a point x on $\mathbf{C}$. Here, a germ is an equivalence class of functions, where f and g are continuous functions in some neighbourhoods of x which

agree in a neighbourhood of x. This is a local ring whose maximal ideal is the germ of those functions which vanish at x.
In number theory, one looks at rings like the p-adic integers for some prime p. This consists of power series $\sum_{n=0}^{\infty} a_n p^n$ where $0 \leq a_n < p$ for all p; power series are added and multiplied and re-written again with 'digits' between 0 and $p-1$. This is completely similar to adding and multiplying usual decimals. This ring is a local ring and its unique maximal ideal consists of all those power series which have no constant term. This is a PID.

We have the following very useful way of producing prime ideals:
Let A be a commutative ring with 1 and S a multiplicatively closed subset not containing 0. Then, there is an ideal P maximal with respect to the property that $P \cap S = \emptyset$. Further, P must be a prime ideal.
Zorn's lemma implies that such a P exists; this is just the inverse image of a maximal ideal of $S^{-1}A$.
If $a, b \notin P$ but $ab \in P$, we have that both $P+(a)$ and $P+(b)$ must intersect S. If $p+au = s \in S$ and $q+bv = t \in S$, then $st = pbv+qau+pq+abuv \in P \cap S$, a contradiction. Thus, P is a prime ideal.

Let us use this to prove :
Nil (A) is the intersection of all prime ideals of A.
First, each nilpotent element $a \in P$ for each prime ideal since $a^r = 0 \in P$ implies $a \in P$. Conversely, suppose that $a \in A$ is not nilpotent. Then, the set of powers $a^i, i \geq 0$ forms a multiplicative subset S of A. Any prime ideal of $S^{-1}A$ is of the form $S^{-1}P$ for some prime ideal P of A which does not intersect S. In other words, a is not in P. This proves the above assertion.
Now, this immediately gives by going to quotient rings, the following assertion :
If $I \subset A$ is an ideal, then its 'radical' ideal $\sqrt{I} := \{x \in A : x^r \in I \; for \; some \; r > 0\}$ is the intersection $\bigcap_{P \supset I} P$ of all prime ideals containing I.
Another application is :
In any A, the set Z of zero divisors contains all the non-zero elements of some prime ideal.
Consider S to be the complement of $Z \cup \{0\}$. It is easy to see that S is multiplicatively closed. Thus, by the above result, there is some prime ideal contained in $Z \cup \{0\}$.
For any ring A, one defines the Jacobson radical Jac (A) to be the intersection of its maximal ideals. Since maximal ideals are prime, we have Jac (A) $\supset$ Nil (A).

In fact, an interesting fact is :
Jac $A[X] = Nil\ A[X]$.
Here is the proof. We need to show that any $f \in$ Jac $A[X]$ is nilpotent. Write $f = \sum_{i=0}^{n} a_i X^i$. Now $1 + Xf$ must be a unit since it cannot be in any maximal ideal of $A[X]$ (as Xf is in each maximal ideal). Thus, by what we proved in the beginning, all a_i are nilpotent. Hence f is nilpotent.

§ 2 *Factorisation in domains*

In this section, we assume that A is an integral domain.
We shall write a/b (and say a divides b) if $ac = b$ for some $c \in A$.

• 2.1 *Euclidean and principal ideal domains*

A domain A is said to be a *Euclidean domain* if it has a Euclidean (division) algorithm i.e., there is a function $d : A \setminus \{0\} \to \mathbf{N}$ such that: (i) a/b implies $d(a) \leq d(b)$ and (ii) $a, b \neq 0$ implies $\exists q, r \in A$ with $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.
Any field K is a Euclidean domain (with $d(a) = 1$ for all $a \neq 0$). So also is $K[X]$ (with d as degree).
For a field K, the formal power series ring $K[[X]]$ is a Euclidean domain with $d(\sum_{i \geq n} a_i X^i) = n$ if $a_n \neq 0$.
It is easy to see that $\mathbf{Z}, \mathbf{Z}[i]$ are Euclidean domains.
It is also easy to see that any Euclidean domain (without assuming that $1 \in A$ to begin with) must contain 1. For, an element a with $d(a)$ minimum among all $d(x)$ for $x \neq 0$, is seen to be 1.

$A = \{a + b\sqrt{3}i : a, b \in \mathbf{Z}\}$ is not Euclidean. Similarly, $\{a + b\sqrt{5}i : a, b \in \mathbf{Z}\}$ is not Euclidean.
Note that to prove a domain is Euclidean, we need only produce some Euclidean size function but to prove that a certain domain is not Euclidean is much more difficult. For, one has to rule out *any* size function d as in the definition. Therefore, not surprisingly, the above two statements will be proved by proving a stronger one viz., that these are not UFDs (to be discussed shortly).

A domain A is a *principal ideal domain* (PID for short) if every ideal is principal i.e., is of the form $\{ax : a \in A\}$ for some x.
For instance, $\mathbf{Z}$ is a PID but $\mathbf{Z}[X]$ is not. Indeed, $A[X]$ is a PID if, and only

if, A is a field as implied by the following :
(i) *Every Euclidean domain (A, d) is a PID. In particular, $\mathbf{Z}[X]$ is not a Euclidean domain.*
(ii) *For a domain A, $A[X]$ is a PID if and only if A is a field.*
Proof.
(i) Let (A, d) be a Euclidean domain. Suppose $I \neq 0$ is an ideal. Let $d(a) = Min\{d(x) : x \in I, x \neq 0\}$. If $b \neq 0$ is in I, then $b = qa + r$ with either $r = 0$ or $d(r) < d(a)$. If $r \neq 0$, this means that $r = b - qa \in I$ and satisfies $d(r) < d(a)$, an impossibility. Thus $r = 0$ i.e., $b \in (a)$. So, $I \subseteq (a) \subseteq I$ i.e., $I = (a)$ i.e., A is a PID.
(ii) Now, if A is a field, then $A[X]$ is a Euclidean domain and hence a PID by (i). Conversely, suppose that A is not a field. If $0 \neq a \in A$ is not a unit, then the ideal (a, X) cannot be principal.

Let $\zeta = e^{2i\pi/23}$. Then, the ring $A_{23} = \{\sum_{i=0}^{21} a_i \zeta^i : a_i \in \mathbf{Z}\}$ is not a PID. This is difficult to prove unless one uses algebraic number theory, and is the main reason that Fermat's last theorem is not trivial to prove for the 23rd power, for instance.
In fact, if we consider for a prime p, the corresponding ring A_p (with p replacing 23 above), then if this ring is a PID, it is elementary to prove that the equation $X^p + Y^p = Z^p$ has only the solutions $XYZ = 0$ in integers. For $p = 23$, it turns out that the ring $A = \{a + b\frac{1+\sqrt{-23}}{2} : a, b \in \mathbf{Z}\}$ is contained in A_{23} and that the nonprincipal ideal generated by 2 and $\frac{1+\sqrt{-23}}{2}$ in A is the intersection of A with a nonprincipal, prime ideal of A_{23}.

If d is a square-free (positive or negative) integer and $D = \sqrt{d}$ or $(1 + \sqrt{d})/2$ according as $d \equiv 2, 3 \bmod 4$ or $\equiv 1 \bmod 4$, then look at the ring $A = \{a + bD : a, b \in \mathbf{Z}\}$. It is still an unsolved conjecture that A is a PID for infinitely many d.

Usual prime integers are characterized by either of the two equivalent properties :
$p|ab$ implies either $p|a$ or $p|b$.
$p = uv$ implies either $u = \pm 1$ or $v = \pm 1$.
Contrastingly, it will be seen that these two properties are not equivalent in more general domains. Therefore, we have the following two notions.
An element a in a ring A is said to be *prime* (respectively *irreducible*) if it is a non-zero, non-unit such that whenever a/bc (respectively, when $a = bc$),

either a/b or a/c (respectively, b or c must be a unit).

In any domain, prime elements are irreducible.
The reason is that if p is prime and $p = ab$, then $p|ab$ and so $p|a$ or $p|b$. Suppose $pc = a$ without loss of generality. Then, $p = ab = pcb$ i.e., $p(1-cb) = 0$ i.e. $1 = cb$. So, b is a unit.

Note that a is a prime if, and only if, the principal ideal (a) is a non-zero prime ideal and that b is irreducible if, and only if, (b) is maximal among non-zero, principal, proper ideals. Thus, *in a PID, all non-zero prime ideals are maximal and prime elements and irreducible elements coincide.*
In particular, if K is a field, then an ideal I of $K[X]$ is maximal if, and only if, $I = (f)$ for some irreducible element f in $K[X]$.

Now, we discuss a number-theoretic application of the above results:

(Corollary of the fact that $\mathbb{Z}[i]$ is a E.D.)
Any prime number $p \equiv 1$ mod 4 is a sum of two square of integers.
Proof:
We first claim that $\exists a$ such that $a^2 \equiv -1 \ mod\ p$.
In fact, we show that $a = \left(\frac{p-1}{2}\right)!$ works. By Wilson's theorem, $(p-1)! \equiv -1 \ mod\ p$.
A simple proof of this is as follows. Multiply out all the elements of the group $\mathbb{Z}_p^*$. Each element cancels off with its inverse except for 1 and $p-1$ which are their own inverses. Thus, this product (which is $(p-1)!$) is just $p-1$ in $\mathbb{Z}_p^*$. Therefore, $(p-1)! \equiv p-1 \ mod\ p$.
But

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot 3 \ldots (p-3)(p-2)(p-1) \\ &= 1 \cdot (p-1) \cdot 2 \cdot (p-2) \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \\ &\equiv (-1^2) \cdot (-2^2) \cdot (-3^2) \ldots \left\{ -\left(\frac{p-1}{2}\right)^2 \right\} \ mod\ p\end{aligned}$$

Thus, the claim is proved.
So, $a^2 + 1 = dp$ for some $d \in \mathbb{Z}$. Now, we view this equation in $\mathbb{Z}[i]$. We have $(a+i)(a-i) = dp$.
If p were irreducible as an element of $\mathbb{Z}[i]$, it would be a prime element since $\mathbb{Z}[i]$ is a Euclidean domain. Since $p/(a+i)(a-i)$ in $\mathbb{Z}[i]$, we would then have $p/(a+i)$ or $p/(a-i)$. Thus $\exists x+iy \in \mathbb{Z}[i]$ such that $p(x+iy) = a \pm i$. This gives $px = a, py = \pm 1$ which is impossible. Therefore, p cannot be irreducible. In

other words, there are $a+bi, c+di \in \mathbb{Z}[i]$ so that $p=(a+bi)(c+di)$ and neither $a+bi$ nor $c+di$ is a unit in $\mathbb{Z}[i]$.
Taking absolute values, we have

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

This implies that either $a^2+b^2=1, c^2+d^2=p^2$ or $a^2+b^2=p=c^2+d^2$ or $a^2+b^2=p^2, c^2+d^2=1$.
The first and the third options do not occur since $a+bi$ and $c+di$ are not units. Thus $a^2+b^2=c^2+d^2=p$.

What we have proved above is that a prime number $p \equiv 1 \bmod 4$ is not a prime element in $\mathbb{Z}[i]$.

For d square-free in $\mathbf{Z}$, let us write θ_d for the set of complex numbers of the form $x=a+b\sqrt{d}$ with $a,b \in \mathbf{Q}$ such that x satisfies a monic polynomial over the integers.
Exercise: Show that θ_d is $\mathbf{Z}[\sqrt{d}]$ or $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ according as $d \equiv 2,3$ mod 4 or $d \equiv 1$ mod 4.
The ring θ_d is called the *ring of integers in* $\mathbf{Q}(\sqrt{d})$.

The following facts require some knowledge of algebraic number theory.

Fact I:
θ_d is a Euclidean domain $\Leftrightarrow$

$$d = -1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$$

θ_d (for $d<0$) is a PID $\Leftrightarrow$

$$-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

Conjecture (Siegel):
There are infinitely many $d>0$ for which θ_d is a PID.

Fact II:
Let p be a prime number, and let $\zeta = e^{2\pi i/p}$. Consider the ring $\mathbb{Z}[\zeta] = \left[\sum_{r=0}^{p-2} a_r \zeta^r : a_r \in \mathbb{Z}\right] \subseteq \mathbb{C}$. If $\mathbb{Z}[\zeta]$ is a PID, then Fermat's equation $X^p+Y^p=Z^p$ has only the trivial solutions $XYZ=0$ in integers X,Y,Z.
Kummer proved that $\mathbb{Z}[\zeta]$ is not a PID for $p=23$. This is why 'Fermat's last theorem' is not trivial.

Fact III:
(Deep) Using the so-called 'generalized Riemann hypothesis' (GRH), it can be proved that for an algebraic number field K whose dimension as a Q-vector space is ≥ 3, the 'ring of integers' of K satisfies θ_K is a ED $\Leftrightarrow$ θ_K is a PID. In fact, if K is a Galois extension of Q and has rank > 3, it has been proved by Harper & Ram Murty without using GRH that $\mathcal{O}_K$ is a PID if and only if it is a Euclidean domain.

The following statement can be deduced quite easily using basic algebraic number theory, but since we have not discussed that theory, the proof below will be somewhat long.

Example of a PID which is not a ED

Consider the ring $A = \mathbb{Z}\left[\frac{1+\sqrt{19}}{2}\right]$. We shall prove that this is a PID and is not a ED. We first show that A is not a Euclidean domain. The proof works more generally as indicated after this . Suppose, if possible, A is a E.D. and $N : A\backslash\{0\} \to \mathbb{Z} \geq 0$ is a size function.
Let $\alpha \in A$ be such that α is not a unit and $N(\alpha) = \min\{N(x) : x \text{ is not a unit }\}$. Now, $\forall x \in A$ we have $x = q\alpha + r$ with either $r = 0$ or $N(r) < N(\alpha)$. So, if $r \neq 0$ then $N(r) = 0$ since $N(r) < N(\alpha)$. But $N(r) = 0 \Rightarrow r$ is a unit.
Let us find the units in A. We claim ± 1 are the only units. Suppose $a + b\theta$ is a unit (where $\theta = \frac{1+\sqrt{-19}}{2}$ for short).
Therefore $1 = (a+b\theta)(c+d\theta) \Rightarrow 1 = (a+b\bar{\theta})(c+d\bar{\theta})$ taking conjugates. Hence

$$1 = (a + b\theta)(a + b\bar{\theta})(c + d\theta)(c + d\bar{\theta}) = (a^2 + ab + 5b^2)(c^2 + cd + 5d)$$

We note that $a^2 + ab + 5b^2 = \frac{(2a+b)^2+19b^2}{4} \geq 0$. Hence $a^2 + ab + 5b^2 = 1 = c^2 + cd + 5d^2$.
Therefore, $(2a + b)^2 + 19b^2 = 4$. If $b \neq 0$, the LHS would be ≥ 19. This $b = 0$ and so $4a^2 = 4$ i.e. $a = \pm 1$. Hence $a + b\theta = \pm 1$ are the only units in A. Therefore, the statement that $\forall x \in A$, we have $x = q\alpha + r$ with either $r = 0$ or r a unit, gives us that the quotient ring $A/(\alpha)$ has atmost three elements (the cosets of $r = 0, 1, -1$). [We note that this goes through for $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ if $d \equiv 1 \ mod\ 4$].

Let us compute $\#(A/(\alpha))$ in another way.
First, $A = \mathbb{Z} + \mathbb{Z}\theta$ is a free abelian group with $\{1, \theta\}$ as a basis [since if $a + b\theta = 0$, then $(a + \frac{b}{2}) + \frac{b}{2}\sqrt{-19} = 0$ i.e. $a = b = 0$] Under the group isomorphism $A \xrightarrow{\pi} \mathbb{Z} \times \mathbb{Z}; a + b\theta \mapsto (a, b)$ let us see what the image of (α) is.

Write $\alpha = a + b\theta$. Then,

$$\begin{aligned}(\alpha) &= \{\alpha\beta : \beta \in A\} = \{(a+b\theta)(c+d\theta) : c, d \in \mathbb{Z}\} \\ &= \{(ac - 5bd) + (ad + bc + bd)\theta : c, d \in \mathbb{Z}\}\end{aligned}$$

since $\theta^2 = \theta - 5$.
Therefore,

$$\begin{aligned}\pi((\alpha)) &= [(ac - 5bd, bc + (a+b)d) : c, d \in \mathbb{Z}] \\ &= \left[\begin{pmatrix} a & -5b \\ b & a+b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} : c, d \in \mathbb{Z}\right].\end{aligned}$$

So,

$$|A/(\alpha)| = |\mathbb{Z}^2/\pi((\alpha))| = \left|\mathbb{Z}^2/\begin{pmatrix} a & -5b \\ b & a+b \end{pmatrix}\mathbb{Z}^2\right| = \left|\det\begin{pmatrix} a & -5b \\ b & a+b \end{pmatrix}\right| = a^2+ab+5b^2.$$

Thus, we have $a^2 + ab + 5b^2 \leq 3$ i.e. $a^2 + ab + 5b^2 = 1, 2$ or 3. In other words, $(2a+b)^2 + 19b^2 = 4, 8$ or 12. This implies $b = 0$ as, otherwise, the LHS ≥ 19. [Note that this carries over with 19 replaced by any $d \geq 13$]. So $4a^2 = 4, 8$ or 12, i.e. $a^2 = 1, 2$ or 3. This gives $a = \pm 1$ i.e. $\alpha = a + b\theta = \pm 1$. This is a contradiction, since α is chosen to be a non-unit of minimal size.
Therefore, A is not a Euclidean domain. *This proof carries over to show that* $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ *for* $d \equiv 3$ *mod* 4 *and* $d > 12$*, is not a Euclidean domain.*
The full list of such quadratic fields was given earlier as fact I.

Now, we prove that $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID. The proof is easy if we use some algebraic number theory but we give an elementary proof.

Idea of proof that A is a PID
If A had been a E.D., the most natural size function we would have thought of is the function $N(a + b\theta) = |a + b\theta|^2$. What we do is to prove that give any $\alpha \neq 0$ in A either an element β is in (α) or $\exists r \in (\alpha, \beta)$ so that $r \neq 0$ and $N(r) < N(\alpha)$.
This would prove that A is a PID, as follows. If I is any ideal, consider $\alpha \in I$ with $\alpha \neq 0$ and $N(\alpha) = \min[N(x) : 0 \neq x \in I]$. If $(\alpha) \neq I$, pick any $\beta \in I, \beta \notin (\alpha)$. By the above, we would get hold of $r \in (\alpha, \beta)$ with $r \neq 0$ and $N(r) < N(x)$. Since $r \in (\alpha, \beta) \subseteq I$, we will have a contradiction. Thus, indeed $I = (\alpha)$.
So, let us now proceed to prove the following:
Let $N : A\backslash\{0\} \to \mathbb{Z}^{\geq 0}; a + b\theta \mapsto |a + b\theta|^2 = a^2 + ab + 5b^2$. If $\alpha \neq 0$ and

$B \notin (\alpha)$, then $\exists r \in (\alpha, \beta)$ with $r \neq 0$ and $N(r) < N(\alpha)$.
Equivalently, we find $a, b \in A$ so that

$$N\left(\frac{\beta a}{\alpha} - b\right) \text{ and } \frac{\beta a}{\alpha} - b \neq 0$$

(then $r = \beta a - \alpha b$ would work).

Let us write $\frac{\beta}{\alpha}$ as $\frac{x+y\theta}{z}$ ($\theta = \frac{1+\sqrt{-19}}{2}$ before see that $\theta^2 = \theta$) where $x, y, z \in \mathbb{Z}, (x, y, z) = 1$ and $z > 0$. Want to find $a = s + t\theta, b = u + v\theta \in A$ so that $\left|\frac{\beta}{\alpha}a - b\right|^2 < 1$.

Now

$$\begin{aligned} \frac{\beta}{\alpha}a - b &= \frac{x + y\theta}{z}(s + t\theta) - u - v\theta \\ &= \frac{(xs + 5ty - uz) + [xt + y(s + t) - vz]\theta}{z} \\ &= \frac{m + n\theta}{z}, \text{ say} \end{aligned}$$

First let us choose s, t, v so that $n = 1$ (can be done $(x, y, z) = 1$). then $\frac{\beta}{\alpha}a - b = \frac{m+\theta}{z}$ with $m = xs - 5ty - uz$. Now, choose $u \in \mathbb{Z}$ such that $\left|\frac{xs-5ty}{z} - u\right| \leq \frac{1}{2}$ i.e. $|m| \leq \frac{z}{2}$.

So

$$\left|\frac{\beta}{\alpha}a - b\right|^2 = \frac{|m + \theta|^2}{z^2} = \frac{m^2 + m + 5}{z^2} \leq \frac{z^2 + 2z + 20}{4z^2}.$$

This is < 1 if $3z^2 - 2z > 20$ which holds if $z \geq 3$. Note that $\frac{\beta}{\alpha} \notin A$ means that $z \geq 2$. If $z = 2$, then either x or y is odd as $\frac{x+yv}{z} = \frac{\beta}{\alpha} \notin A$. So, the above choice of s, t, u, v works if $z \geq$

If $z = 2$, then again look at $\frac{\beta}{\alpha}a - b = \frac{m+n\theta}{z}$, where $m = xs - 5ty - uz$ and $n = xt + y(s + t) - vz$. Now, choose $s + t = x, t = -y$ and $v = 0$ so that $n = 0$. Then $m = x^2 + xy + 5y^2 - 2u$ (remember $z = 2$). So, since either x or y is odd, m is odd, no matter what u is. Choose u so that $m = 1$. Then $\left|\frac{\beta}{\alpha}a - b\right|^2 = \left|\frac{m}{n}\right|^2 < 1$.
This completes the proof.

• 2.2 *Unique factorisation domains*

A domain A is called a *unique factorisation domain* (UFD for short) if, and only if, each non-zero element is uniquely (i.e. upto units) a product of a

unit and finitely many irreducible elements.
It is easy to see in any domain A that an element a is irreducible if, and only if, the principal ideal (a) is maximal among principal, proper ideals. Using this easy observation, it is also easy to see that in any PID, irreducible elements and prime elements are the same. Further, it is equally easy to note that a factorisation domain (that is, a domain in which each nonzero, nonunit can be expressed as a finite product of irreducible elements) has unique factorisation if, and only if, all irreducible elements are prime. The phrase 'irreducible polynomial' should be understood as meaning an irreducible element of the corresponding polynomial ring. For instance, the polynomial $2X$ is **not** an irreducible element in $\mathbf{Z}[X]$ although it is so in $\mathbf{Q}[X]$. These simple remarks are extremely useful as we shall soon see.

Every PID is a UFD.
For the proof, one needs Zorn's lemma. Recall what Zorn's lemma asserts. If a partially ordered set satisfies the property that any totally ordered subset has an upper bound, then there is an element in the original set which is maximal with respect to the partial order. Let A be a PID and suppose, if possible, there are non-zero elements in A which are not expressible as finite products of irreducible elements. Consider the non-empty set Ω of all such elements and the set $\Sigma = \{(a) : a \in \Omega\}$ of the corresponding principal ideals. Inclusion of ideals defines a partial order on Σ. Also, if $\mathcal{C}$ is any totally ordered subset of Σ, let us look at the ideal $I_0 = \bigcup_{I \in \mathcal{C}} I$. If $I_0 = (a_0)$, then $a_0 \in I$ for some $I \in \mathcal{C}$. Thus, $I_0 = I$ i.e., I is an upper bound for $\mathcal{C}$. Applying Zorn's lemma, Σ has a maximal element, say (a). As $a \in \Omega$, a is not irreducible. Suppose $a = bc$ where b and c are non-zero non-units. Then, clearly (a) is properly contained in (b) as well as in (c). By maximality, $c, b \notin \Omega$. In other words, both b and c are finite products of irreducible elements. Thus, $a = bc$ is also so, which contradicts the fact that $a \in \Omega$. Therefore, we have shown that Ω is empty. Finally, the uniqueness is a consequence of the remark above.

In the following paragraph, we allow A to be any commutative ring with unity. Then, we have the following characterisation for a ring to have only principal ideals :
Let A be a commutative ring with unity. Suppose that all prime ideals are principal. Then, all ideals in A are principal.
Proof.

Suppose there do exist non-principal ideals in A. Partially order the set of such ideals by inclusion. If $I_\lambda; \lambda \in \Lambda$ is a totally ordered subset of these, then their union I_0 is clearly also another such ideal. By Zorn's lemma, there is an ideal M which is maximal with respect to the property that it is not principal. Since M cannot be prime by the hypothesis, there are $a, b \notin M$ so that $ab \in M$. Thus, the ideals $M + (a) = (x)$ and $M + (b) = (y)$ for some $x, y \in A$. Expressing x and y in the form $m_1 + aa_1$ and $m_2 + bb_1$ respectively, we notice that $xy \in M$ while $x, y \notin M$. Consider the ideal $(M : (x)) = \{t \in A : tx \in M\}$. This is a proper ideal (as 1 is not in it) which properly contains M as it contains y as well. Thus, $(M : (x)) = (z)$ for some z. If $m \in M \subset M + (a) = (x)$, we write $m = xx_1$ and thus, $x_1 \in (M : (x)) = (z)$ i.e., $x_1 = zz_1$ for some z_1. Thus, $M = (xz)$, a principal ideal. This is a contradiction which proves that there are, indeed, no non-principal ideals.

Cohen's theorem.
(Here is a variant of the above argument to show:)
If, in a ring, all prime ideals are finitely generated, then the ring must be Noetherian (that is, all ideals must be finitely generated).
Proof.
Let P be an ideal, maximal with respect to the property it is not finitely generated. Let $ab \in P$ and $a, b \notin P$. Write $P + (a) = (x_1, \cdots, x_r), P : (a) = (z_1, \cdots, z_s)$. If $x_i = p_i + aa_i$, then it is easy to see that

$$P = (p_1, \cdots, p_r, az_1, \cdots, az_s).$$

In a UFD, irreducible elements and prime elements are the same.
Let us see why. We already know that prime elements are irreducible in any domain. Conversely, let p be an irreducible element in a UFD A. If p/ab, then $pc = ab$ for some c. Expressing a, b, c as products of irreducibles, the uniqueness of decomposition into irreducibles shows that p is, upto a unit, an irreducible factor of a or of b. Thus, $p|a$ or $p|b$ i.e., p is prime.

From this one can observe that $\{a+b\sqrt{3}i : a, b \in \mathbf{Z}\}$ and $\{a+b\sqrt{19}i : a, b \in \mathbf{Z}\}$ are not UFDs.
To see this for the first ring $\mathbf{Z}[\sqrt{-3}]$, note that the only units are 1 and -1 since these are the only solutions of $a^2 + 3b^2 = 1$. Moreover, $1 + \sqrt{3}i$ is not a prime since it divides $(1 + \sqrt{3}i)(1 - \sqrt{3}i) = 4 = 2 \times 2$ while it does not divide

2. We show that $1+\sqrt{3}i$ is irreducible. If not, write $1+\sqrt{3}i = (a+b\sqrt{3}i)(c+d\sqrt{3}i)$. Taking the squares of absolute values, we have $4 = (a^2+3b^2)(c^2+3d^2)$ which has only the solutions $a+b\sqrt{3}i = \pm 1$ or $c+d\sqrt{3}i = \pm 1$. Hence, the ring $\mathbf{Z}[\sqrt{-3}]$ is not a UFD. A similar proof works for $\mathbf{Z}[\sqrt{-19}]$.

The domain of all complex entire functions is not a UFD.
In fact, this is a domain which does not have factorisation. For, the irreducible elements are simply the linear polynomials and evidently there are entire functions which are not polynomials.
The ring $A = \{\sum_{i=0}^{n}(a_i Cosix + b_i Sinix) : a_i, b_i \in \mathbf{R}, a_n b_n \neq 0, n \geq 0\} \cup \{0\}$ is not a UFD. (Here, each element of A is a real, trigonometric polynomial of some degree). The reason for this is an equation like $Cos^2(x) = (1+Sinx)(1-Sinx)$ holds.
In fact, this ring is also realised as $\mathbf{R}[X,Y]/(X^2+Y^2-1)$.
Contrastingly, note that $\mathbf{C}[X,Y]/(X^2+Y^2-1)$ is even a PID. The reason is that it is isomorphic to $\mathbf{C}[Z,1/Z]$ under the isomorphism $Z \mapsto X+iY$.

Interesting Remark
Let $K \supseteq Q$ be an 'algebraic number field' i.e., a field which has finite dimension as a Q-vector space (e.g. $K = Q(\sqrt{d}), K = Q(\zeta)$). Let $\mathcal{O}_K$ denote the 'ring of integers of K' i.e., $\mathcal{O}_k \stackrel{d}{=} [x \in K : x$ satisfies a monic, integral polynomial. Then, $\mathcal{O}_K$ is a PID $\Leftrightarrow$ $\mathcal{O}_K$ is a UFD.
This can be proved quite easily using basic algebraic number theory (for quadratic fields, see a proof in M. Artin's 'Algebra').

(Gauss's theorem)
A is a UFD if, and only if, $A[X]$ is a UFD.

The nontrivial part of the theorem is the implication that if A is a UFD, then $A[X]$ is a UFD as well. Let us assume that A is a UFD. Once again, it is easy to prove that every element of $A[X]$ is a finite product of irreducibles. The nontrivial part is really the uniqueness of the expression. For showing uniqueness, the idea is to go to the quotient field K of A and use the fact that $K[X]$ is a UFD. Let us prove uniqueness.

We need the notion of content of any $f \in A[X]$. This is simply the GCD $c(f)$ of all the coefficients of f and is well-defined up to units (just as the GCD of integers is well-defined up to sign). One can also define the ideal $(c(f))$ to be the smallest principal containing the ideal generated by the coefficients of f. Now, $f = c(f)f_0$ for some $f_0 \in A[X]$ which is 'primitive' i.e., $c(f_0)$ is a unit.

Notice also that irreducible elements in $A[X]$ must be primitive. The proof will use an observation and a lemma due to Gauss. First, we notice :

Observation : $c(fg) = c(f)c(g)$.
To see this, it suffices to show that if $c(f) = c(g) = 1$, then $c(fg) = 1$. If $c(fg) \neq 1$, let p be an irreducible divisor of $c(fg)$. Write $f = \sum_{i=0}^{l} a_i X^i, g = \sum_{i=0}^{m} b_i X^i$. Since $c(f) = 1 = c(g)$, there are a_r, b_s such that $p \not| a_r$, $p \not| b_s$ and $p|a_i, b_j$ for $i < r, j < s$. But, since p divides each coefficient of fg, it divides the coefficient of X^{r+s} in fg. This is a sum of terms each of which is a mutiple of p except possibly for $a_r b_s$. Thus, p must divide $a_r b_s$ which contradicts the fact that p is irreducible (= prime).
The second piece required is:
Gauss's lemma : If $f \in A[X]$ is primitive, then it is irreducible in $A[X]$ if, and only if, it is irreducible in $K[X]$.
For this, write, if possible, $f = gh$ with $g, h \in K[X]$. Rewrite it as $f = \frac{a}{b} g_0 h_0$ with $g_0, h_0 \in A[X]$ primitive and a, b coprime. So, $bf = ag_0 h_0$. Comparing contents, we get $a = b\times$ unit and, $c(f) = \frac{a}{b}$. So, $f = c(f)g_0 h_0 = g_0 h_0$ which means that f is reducible in $A[X]$, which is a contradiction. This proves Gauss's lemma.
Finally, let us prove uniqueness of factorisation. As observed earlier also (see the remarks before the proof of the fact that PIDs are UFDs), since factorisation holds, the uniqueness follows if one checks that irreducible elements are also prime. To show this, let $f \in A[X]$ be an irreducible element. Suppose f/gh in $A[X]$. Now, by Gauss's lemma, f is irreducible in $K[X]$ and so it is a prime element of $K[X]$ as $K[X]$ is a UFD. Thus, suppose $fg_0 = g$ where $g_0 \in K[X]$. Write $g_0 = \frac{a}{b} g_1$ with $a, b \in A$ coprime and $g_1 \in A[X]$ primitive. So, $bg = bfg_0 = afg_1$. Comparing contents and noting that $c(f) = 1$ as it is irreducible in $A[X]$, we have $a = bc(g)$. Thus, $bg = afg_1 = bc(g)fg_1$ i.e., $g = c(g)fg_1$ i.e., f/g in $A[X]$. Hence f is indeed a prime element of $A[X]$. The proof of Gauss's theorem is complete.

Corollary.
Let α be an algebraic integer. Then, $min(\alpha, \mathbf{Q})$ is in $\mathbf{Z}[X]$ where $min(\alpha, \mathbf{Q}) :=$ the monic polynomial of smallest degree in $\mathbf{Q}[X]$ satisfied by α.
In particular, $\mathbf{Z}[\alpha] \cong \mathbf{Z}[X]/(min(\alpha, \mathbf{Q}))$.

Over a field K, the ring $K[[X]]$ of formal power series is a UFD as we already saw that it is a Euclidean domain. More directly, the proof can be seen as follows. Clearly, any power series can be written as $f = \sum_{n=r}^{\infty} a_n X^n$ with

$a_r \neq 0$ for some $r \geq 0$. One may call r, the order of f. Note that a power series over K is invertible if, and only if, its constant term is zero. Hence, each element $f \in K[[X]]$ is uniquely expressible as $X^r u$ for some $r \geq 0$ and some unit $u \in K[[X]]^*$. So, it is clear that upto units, the only irreducible element is X. The question of uniqueness of decomposition into irreducibles is equivalent to the question as to whether the order r is determined by f. This is evidently true. Hence $K[[X]]$ is a UFD.
A word of warning is that the analogue of Gauss's theorem is false; that is, *there are UFDs A for which $A[[X]]$ are not UFDs.* If A is a PID, then $A[[X]]$ is a UFD (a proof can be given using Nagata's criterion below).

Here is another interesting criterion for UFDs :
Let A be a domain in which each non-zero prime ideal contains a prime element. Then, A is a UFD.
To prove this, one just needs to show that each non-zero, non-unit $a \in A$ is expressible as a finite product of prime elements (for this implies uniqueness in terms of irreducibles). Now, the set S of such elements along with the set of units is a multiplicatively closed subset. In fact, S is saturated (that is, $ab \in S$ if and only if $a, b \in S$). If $a \neq 0$ is not in S, then (a) does not intersect S. Choosing a prime ideal P containing (a), not intersecting S, there is a prime element $p \in P$; this would contradict the fact that $p \in S$. Hence $A - S = (0)$. So, each non-zero, non-unit a is expressible as a finite product of prime elements.

Exercise: S is saturated if and only if $A - S$ is a union of prime ideals.

We have the following useful observation :
If A is a UFD, then so is $S^{-1}A$ for any localisation.
Indeed, any prime $a \in A$ is either a divisor of an element of S (and so, becomes a unit in the localisation) or remains a prime in the localisation. Note also that A injects into ${}^{-1}A$ and any non-zero, non-unit in $S^{-1}A$ is associate (in this localisation) to an element of A. Since elements of S are products of primes in A, each non-zero, non-unit of $S^{-1}A$ is a product of prime elements (easy) and this shows $S^{-1}A$ is a UFD.

Nagata's criterion for UFD's
If R is a domain and S is a multiplicative subset generated by a certain set of prime elements, and if R_S is a UFD, then A itself is a UFD.
Proof.
Since R is a FD, enough to show that every irreducible element $p \in R$ is

prime. Let p be irreducible in R. The fact that S is generated by primes, shows easily:
Claim (i): S is saturated (i.e., $ab \in S$ iff both a, b are in S).
Let us also grant:
Claim (ii): Either p remains irreducible in R_S or p divides some element of S (and so, becomes a unit in R_S).
Proof continued modulo claims
Case 1: p remains irreducible.
Then p is prime in R_S, i.e., pR_S is a prime ideal But $pR_S = I_S$ where $I = pR$. Thus I is a prime ideal in R. That is, p is prime in R itself.
Case 2: p becomes a unit.
Then Rp intersects S. Since S is saturated, $p \in S$. So p is a product of n prime factors (not necessarily distinct). As p is irreducible, we have $n = 1$. That is, p is prime.
To prove claim (ii), note if $a = (b/s)(c/t)$ for $b, c \in R$, and $s, t \in S$, then $sta = bc$. Now st is a product of primes in R; so each prime divides b or c. By repeated cancellation (in R), eventually arrive at $a = de$ where $d = b/u, e = c/v$ where d, e are in R and u, v are in S. This shows either d or e is a unit in R (as a is irreducible in R). So either b or c is a unit in R_S. So a remains irreducible in R_S (if one of b, c is a unit in R_S) or becomes a unit (if both b, c are units in R_S).

Corollary (application of Nagata)
The coordinate ring $\mathbf{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$ of the real unit sphere is a UFD.

Remarks and exercises.

1. *Let $A \subset B \subset K = Q(A)$ where A is a PID and B is a subring of K containing* 1. *Then B is a PID.*

Proof.

Let $0 \neq I \subset B$ be an ideal. Write $I \cap A = Aa$. Let $0 \neq u/v \in I$ be any non-zero element. Now $uA + vA = wA$ say. Write $u = sw, v = tw, w = cu + dv$. Then $cs + td = 1$. So $\frac{1}{t} = cs/t + d = cu/v + d \in B$. Now $s = t(s/t) = t(u/v) \in I \cap A = Aa$. So, $u/v = (1/t)s \in B(Aa) = Ba$. Thus, $I = Ba$.

2. *$x^2 + 1 = y^3$ has only the solutions $x = 0, y = 1$ in integers.*

Proof.

Let x, y be a solution. Clearly, x even and y odd. If π is an irreducible element of $\mathbf{Z}[i]$ dividing both $x + i$ and $x - i$, then $|\pi|^2$ is an integer dividing (in $\mathbf{Z}[i]$) both $2i$ as well as the odd integer y, which is a contradiction. Hence $x+i, x-i$ are both cubes (up to units) in the Gaussian ring. As all the units here are cubes, we have $x + i = (a + ib)^3$. Unwind to get the result.

3. *The equation $x^2 + 2 = y^3$ has only the solutions $(\pm 5, 3)$.*

The proof is similar working with the Euclidean domain $\mathbf{Z}[\sqrt{-2}]$.

4. *A prime $p \neq 3$ is of the form $x^2 + 3y^2$ if and only if $p \equiv 1$ mod* 3.

Proof.

Clearly, if $p \neq 3$ is of the form $x^2 + 3y^2$, then it is 1 mod 3. Conversely, let $p \equiv 1$ mod 3. So, 3 divides $\mathbf{F}_p^*$ and, hence there exists $a \not\equiv 1$ mod p but $a^3 \equiv 1$ mod p. Thus, p divides a^2+a+1 so that p divides $|-a+\omega|^2$. Clearly, p is not irreducible (therefore, not prime) in $\mathbf{Z}[\omega]$. Hence $p = (a+b\omega)(c+d\omega)$ which are not units, which gives $p = |a + b\omega|^2 = a^2 - ab + b^2$. Therefore, either a, b are both odd or one of them (say a) is odd and the other even, In the first case, $p = ((a + b)/2)^2 + 3((a - b)/2)^2$ and, in the 2nd case, $p = (a - b/2)^2 + 3(b/2)^2$.

5. $\mathbf{Z}[2i]$ is not a UFD because $X^2 + 1$ is a reducible polynomial over the quotient field but irreducible in $\mathbf{Z}[2i]X$.

Similarly, $\mathbf{Z}[\sqrt{8}]$ is not a UFD as seen by considering $X^2 - 2$.

6. $\mathbf{Z} + X\mathbf{Q}[X]$ is not a UFD.

Indeed, X is not a product of irreducibles! The only irreducibles are $\pm$ primes and irreducible polynomials of the form $\pm 1 + Xf$.

7. $X^3 + X + 1$ is irreducible in $\mathbf{Z}[X]$ as it is so in $\mathbf{Z}_2[X]$.

8. $X^4 + 1$ is irreducible over $\mathbf{Z}$ but reducible modulo each prime! (will

not prove this latter fact here). Irreducibility over integers is checked by Eisenstein after changing X to $X+1$.

9. $X^{10} - 6iX^7 + 8X^3 - 1 + 3i$ is irreducible in $\mathbf{Z}[i][X]$.
Indeed, apply Eisenstein with the prime $1+i$.
$X^n - p$ is also irreducible in the above ring for any odd prime number p.
Indeed, p is already prime if it is 3 mod 4. If it is 1 mod 4, take an irreducible factor of it in the Gaussian ring.

10. $\mathbf{R}[X,Y]/(X^2+Y^2-1), \mathbf{C}[X,Y,Z]/(X^2+Y^2+Z^2-1)$ *are not UFDs.*
(Compare with the earlier application of Nagata criterion that the co-ordinate ring of the real 2-sphere is a UFD.)
As $X.X = 91+Y)(1-Y)$ in the former case and $(X+iY)(X-iY) = (1+Z)(1-Z)$ in the latter case, the first two statements follow.

11. $X^{100} - 123123X^{28} + 110$ *cannot take the values* ± 33 *over integers.*
Indeed, apply Eisenstein for the prime 7 or 11 for ruling out 33 and for the prime 11 or 13 to rule out -33.

12. $\mathbf{Z}[\sqrt{-d}]$ is not a UFD for any square-free integer $d \geq 3$.
If d is odd, $(1+\sqrt{-d})(1-\sqrt{-d}) = 2((1+d)/2)$.
If d is even, $(2+\sqrt{-d})(2-\sqrt{-d}) = 2(2+\frac{d}{2})$.

13. *The algebraic integers in* $\mathbf{Q}[\sqrt{d}]$ *for a square-free integer* d *consists of* $\mathbf{Z}[\sqrt{d}]$ *or* $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ *according as to whether* $d \equiv 2, 3$ *mod* 4 *or* $d \equiv 1$ *mod* 4.
Proof.
The minimal polynomial of an algebraic integer $\alpha = a + b\sqrt{d}$ must be in $\mathbf{Z}[X]$ which gives $2a, a^2 - db^2 \in \mathbf{Z}$.
If a is not an integer, write $2a = a_1$ an odd integer. Now, writing $b = b_1/c_1$ we have

$$a_1^2 c_1^2 - 4db_1^2 \in 4c_1^2\mathbf{Z}$$

since $a^2 - db^2 \in \mathbf{Z}$.
So, $4/c_1^2$ and $c_1^2/4d$. Clearly then c_1 is even and thus it must be equal to 2 (otherwise d is not square-free). In other words, both a, b are half-integers which are not integers.
As $4a^2 - 4db^2 = a_1^2 - db_1^2$ is a multiple of 4, d must be 1 mod 4 in case a is not an integer. Thus, $d \equiv 2, 3$ mod 4 cases are done. If $d \equiv 1$ mod 4, then noting that $(1+\sqrt{d})/2$ is an algebraic integer, we are done.

14. *In a Euclidean algorithm* δ *in a Euclidean domain, the quotient and*

remainder are all unique if and only if $\delta(a+b) \leq max(\delta(a), \delta(b))$.
Proof.
If $\delta(a+b) > \delta(a), \delta(b)$ for some $0 \neq a, b$ then the two divisions

$$b = 0(a+b) + b$$

$$b = 1(a+b) - a$$

are valid (as $\delta(b), \delta(-a) < \delta(a+b)$) and give different quotients and remainders.
Conversely, let $a = qb+r = q'b+r'$ with q, q' different or r, r' different. Then, $(q-q')b = r - r'$ gives a contradiction in case $\delta(r-r') \leq max(\delta(r), \delta(-r'))$.

15. *In* $\mathbf{Z}[\sqrt{-7}]$*, for each* $k \geq 2$*, there is an element which is a product of* $2k, 2k+1, \cdots, 3k$ *irreducible elements at the same time!*
Proof.
$8 = 2.2.2 = (1-\sqrt{-7})(1+\sqrt{-7})$. Raise it to the k-th power and keep replacing $(1-\sqrt{-7})(1+\sqrt{-7})$ by 2.2.2.

16. *Express* $43i - 19$ *as a product of irreducibles in* $\mathbf{Z}[i]$.
Indeed, $43^2 + 19^2 = 2210 = 17.13.5.2$. As $4 \pm i, 2 \pm 3i, 2 \pm i, 1 + i$ and their associates are the irreducible factors, we need to pick from them. It turns out that

$$43i - 19 = (4-i)(2+3i)(2+i)(1+i)$$

17. *The quotient field of* $K[[X]]$ *is the Laurent series field* $K((X)) := \{\sum_{n \geq -N} \alpha_n X^n\}$.
Note that the quotient field of $\mathbf{Z}[[X]]$ *is strictly contained in that of* $\mathbf{Q}[[X]]$*; for example,* e^X.

18. *If* $I + J = A$ *(*A *commutative with unity), and if* IJ *is an* n*-th power of an ideal, then so are* I *and* J.
Proof.
Let $IJ = R^n$. Now $I^r + J^r = A$ for all $r \geq 1$ (c0nsider $(x+y)^{2r}$ where $x + y = 1$ in $I + J = A$).
In particular, $I^{n-1} + J = A$.
Then $(I+R)^n = I^n + I^{n-1}R + \cdots + R^n = I(I^{n-1} + \cdots + J) = IA = I$.

19. *Let* $p > 2$ *be a prime. Then* -2 *is a square mod* p *if and only if* $p \equiv 1$ *or* 3 *mod* 8*. From this, it follows that a prime* $p \equiv 1, 3$ *mod* 8 *if and only if*

$p = x^2 + 2y^2$ *for some integers* x, y.
Proof.
The nontrivial part is to show that if $p \equiv 1$ or $3 \bmod 8$, then -2 is a square mod p. Let $a \in \mathbf{F}_{p^2}^*$ have order 8. Then, $a + a^3$ clearly satisfies $(a+a^3)^p = a+a^3$ (that is, $a+a^3 \in \mathbf{F}_p$) and $(a+a^3)^2 = -2$. Therefore, there exists an integer b such that $p|(b^2+2)$. Then, use the fact that $\mathbf{Z}[\sqrt{-2}]$ is a UFD (as it is a ED).

20. *If A is a Boolean, commutative ring (not assumed to have unity), then each finitely generated ideal is principal.*
Indeed, $(a, b) = (a + b - ab)$.

21. *For a polynomial $f \in A[X]$ (with A commutative ring with unity), define the polynomial f' in an obvious manner. Then, f has a multiple root α in some ring B containing A if and only if $f'(\alpha) = 0$.*

22. *The only idempotent elements in a local ring are* $0, 1$.
In fact, if $e(1-e) = 0$, then exactly one of e and $1-e$ is in the maximal ideal. If e is in it, then $1 - e$ is a unit which means that $0 = e(1-e)(1-e)^{-1} = e$.

Here is another nice application of the fact that $K[t]$ is a UFD for any field K. This is the analogue of Fermat's last theorem. We have:
Let $n \geq 3$ be not divisible by the characteristic of K. Then, for any $a, b, c \in K^*$, there are no solutions of $af^n + bg^n = ch^n$ for coprime nonconstant polynomials $f, g, h \in K[t]$.
To prove this, we observe that we may assume K is algebraically closed. Further, since n is not a mutiple of Char. K, one can extract n-th roots of a, b, c in K^* and thus we may assume that $a = b = c = 1$. The coprimality assumption means clearly that they are pairwise relatively prime. Also, evidently this is equivalent to the assumption that the sets of roots of f, g, h are disjoint. Now, let us say deg g is maximal among the three and let us write the equation $f^n + g^n = h^n$ as

$$f^n = \prod_{i=1}^{n} (h - \zeta^i g)$$

where $\zeta = e^{2i\pi/n}$.
If $h - \zeta^i g$ and $h - \zeta^j g$ have a common root s for some $i \neq j \leq n$, then $g(s) = 0 = h(s)$, a contradiction. Hence $h - \zeta^i g, i \leq n$ are pairwise coprime.

Since $K[t]$ is a UFD, we must have

$$h - \zeta^i g = c_i f_i^n$$

for some $c_i \in K$ and $f_i \in K[t]$. Now, since $n \geq 3$, the three polynomials $h - \zeta^i g$ for $i = 0, 1, 2$ are distinct, and hence, there is a linear dependence relation between them since they are in the two-dimensional vector space spanned by g, h. Such a relation clearly gives a relation of the form

$$a_1 f_1^n + a_2 f_2^n + a_3 f_3^n = 0.$$

Once again, we may take n-th roots of the a_i's and we have an identity of the form

$$g_1^n + g_2^n = g_3^n$$

where deg g_i = deg $f_i \leq$ (deg g/n). Thus, we may apply induction on the maximal degree deg g to prove the result.

We observed in UFDs that there are natural notions of the GCD and the LCM of a finite set of elements. These were defined as they are done for integers in terms of prime numbers - here one uses the prime elements. Of course, the GCD and LCM are defined only upto units; this is also just as in $\mathbf{Z}$, where these are defined upto sign. Moreover, in integers, the GCD of a and b is expressible as $ax + by$. This is true in PIDs but not true in general UFDs. For instance, in $K[X, Y]$, where K is a field, X and Y are coprime but there is no relation of the form $1 = Xf + Yg$ in $K[X, Y]$.
In a general integral domain, the GCD or LCM may not exist. We ask the following questions (the following discussion is due to Dinesh Khurana and appears in an article in Resonance) :
Q 1. *Does the existence of GCD of two elements in a domain imply the existence of their LCM?*

Q 2. *Does the existence of LCM of two elements in a domain imply the existence of their GCD?*
While the answer to the second question is in the affirmative, the answer to the first one is in the negative. In fact, we show the existence of two elements in each $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$ an integer, which have a GCD but fail to have an LCM. As we observed above that in a UFD any two elements have an LCM, it follows immediately that $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$ is not a UFD. It is well known that $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-2}]$ are UFDs (in fact, they are even Euclidean domains).

In $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$, we also use the proof to exhibit an irreducible element which is not prime. This again reproves that $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$, is not a UFD.

Before going into our proof, we point out an important fact. In number theory, one studies the rings $\mathbf{Z}[\sqrt{d}]$ for square-free d. Note that any element of this ring is $u = a + b\sqrt{d}$ which is a root of the polynomial $(X-a)^2 - db^2$; this is a polynomial which has integer coefficients and is monic (i.e., has top coefficient 1). Such complex numbers go under the name of *algebraic integers*. Thus, elements of $\mathbf{Z}[\sqrt{d}]$ are algebraic integers. However, in number theory one actually needs to study the set of *all* the algebraic integers in a particular number field like $\mathbf{Q}[\sqrt{d}]$. In $\mathbf{Q}[\sqrt{d}]$, which consists of all complex numbers of the form $s + t\sqrt{d}$ with s, t rational numbers, the ring of all algebraic integers may be larger than $\mathbf{Z}[\sqrt{d}]$. For instance, for $d = -3$, the number $\frac{1}{2} + \frac{\sqrt{-3}}{2}$ is also an algebraic integer. Indeed, the ring of algebraic integers in $\mathbf{Q}[\sqrt{d}]$ is $\mathbf{Z}[\sqrt{d}]$ or $\mathbf{Z}[(d+\sqrt{d})/2]$ according as whether $d \equiv 2$ or 3 mod 4 or as $d \equiv 1$ mod 4. One calls the set of all algebraic integers in $K = \mathbf{Q}[\sqrt{d}]$ the *ring of integers of* K. It was proved by Gauss that the ring of integers of quadratic field $\mathbf{Q}[\sqrt{-d}]$ is a UFD for $d = 1, 2, 3, 7, 11, 19, 43, 67$ and 163. Gauss also conjectured that for no other positive d is the ring of integers of $\mathbf{Q}[\sqrt{-d}]$ a UFD. This conjecture was proved, after about 150 years, in 1966 by Baker and Stark independently. As the ring of integers of $\mathbf{Q}[\sqrt{-d}]$ is $\mathbf{Z}[\sqrt{-d}]$ if $d \equiv 2$ *or* $3(mod\ 4)$, so an easy proof of Gauss conjecture follows in these two cases.

The first observation is:
Let D be an integral domain and $a, b, r \in D$. If (ra, rb) exists then (a, b) exists and $r(a, b) = (ra, rb)$.
Here is the proof. As r divides both ra, rb, $g = (ra, rb)/r$ is in D. Now as (ra, rb) divides ra and rb, g divides a and b. Now if d divides a and b, then dr divides ar and br and thus dr divides (ar, br). This implies that d divides $(ar, br)/r$.

The second observation is:
Let $a, b \in D$. Then $[a, b]$ exists if and only if (ra, rb) exists for all $r \in D$.
Here is the proof. Suppose $[a, b]$ exists. We show that $d := ab/[a, b]$ equals (a, b). As $a = d[a, b]/b$ and $b = d[a, b]/a$, d divides both a and b. Now suppose that h is a common divisor of a and b. Now as a, b both divide ab/h, $[a, b]$ divides ab/h which implies that h divides $ab/[a, b] = d$. Thus if $[a, b]$ exist then so does (a, b) and equals $ab/[a, b]$.

Now we show that if $[a,b]$ exists then so does $[ra,rb]$ for all in D. First note that ra, rb both divide $r[a,b]$. Now suppose m is a common multiple of ra, rb. Then r divides m and a, b both divide m/r. Thus $[a,b]$ divides m/r and so $r[a,b]$ divides m. Thus $[ra,rb] = r[a,b]$.
Now, we claim that if (ra,rb) exists for all r, then $[a,b]$ exists and equals $l := ab/(a,b)$. Clearly a, b both divide l. Now suppose a, b both divide m. Then ab is a common divisor of ma and mb and so ab divides $(ma,mb) = m(a,b)$ by the earlier result above. This implies that $ab/(a,b)$ divides m. Thus, we have :
If $[a,b]$ exists then (a,b) exists and $[a,b](a,b) = ab$.

Let us now prove :
In each $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$ an integer, there exist two elements a, b such that (a,b) exists but $[a,b]$ does not exist. In particular, $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$, is not a UFD.
Proof.
First suppose that $d+1$ is not a prime number. Let $d+1 = pk$, where p is a prime and $k \geq 2$. Clearly $a^2 + db^2 \neq p$ for any $a, b \in \mathbf{Z}$ because the left hand side is bigger than p if $b \neq 0$. If $p = (a + b\sqrt{-d})(u + v\sqrt{-d})$ in $\mathbf{Z}[\sqrt{-d}]$, then taking complex conjugates we see that $u = a, v = -b$. Thus, $p = a^2 + db^2$, which is impossible as observed above. Therefore, p is an irreducible element in $\mathbf{Z}[\sqrt{-d}]$. Also p does not divide $1 + \sqrt{-d}$ because $p(a+b\sqrt{-d}) = 1+\sqrt{-d}$ gives $pa = 1$ which is impossible. Thus, $(p, 1+\sqrt{-d})$ exists and equals 1. We shall show that $(pk, (1 + \sqrt{-d})k)$ does not exist. If it did, then by the first observation, $(pk, (1 + \sqrt{-d})k) = k$. Then as $1 + \sqrt{-d}$ divides $pk = 1 + d$ and $(1 + \sqrt{-d})k$, $1 + \sqrt{-d}$ divides k. Let $k = (1 + \sqrt{-d})(a + b\sqrt{-d}) = (a - bd) + (a + b)\sqrt{-d}$. This gives $a = -b$ and $a - bd = a + ad = k$. Thus $apk = a(1 + d) = k$ which is a contradiction. In view of the second observation, it follows that $[p, 1 + \sqrt{-d}]$ does not exist.

Now suppose that $d+1$ is a prime. Then d and $d+4$ are even integers. Let $d + 4 = 2k$, for some $k > 1$. As above, one easily checks that 2 is irreducible and 2 does not divide $2 + \sqrt{-d}$. Thus $(2, 2 + \sqrt{-d})$ exists and equals 1. We show that $(2k, (2 + \sqrt{-d})k)$ does not exist. If it did, then as above, $2 + \sqrt{-d}$ divides k and which in turn implies that $4 + d$ divides $k = (4 + d)/2$ in $\mathbf{Z}$. This contradiction shows by above that $[2, 2 + \sqrt{-d}]$ does not exist.

In the above proof, note that when $d+1 = pk$, p divides $d+1 = (1+\sqrt{-d})(1-\sqrt{-d})$ but p clearly does not divide either of $1 + \sqrt{-d}$ and $1 - \sqrt{-d}$, showing

that p, which is irreducible, is not prime. Similarly in the second part of the proof, 2 divides $d+4 = (2+\sqrt{-d})(2-\sqrt{-d})$ but does not divide either of them, which shows that 2 is not prime. This also proves that $\mathbf{Z}[\sqrt{-d}]$, $d \geq 3$, is not a UFD.

A general criterion available to check irreducibility of a polynomial over a UFD is the Eisenstein criterion. Even over $\mathbf{Z}$, this is the only general criterion. However, before stating and proving it, we mention a very simple but important general method of concluding that an integral polynomial is irreducible. This works 'by hand'. To illustrate it, consider the polynomial $p(X) = X^4 + 3X^2 + 7X + 4$. Modulo 2, we have $p(X) = X(X^3 + X + 1)$ and both factors are irreducible over the field $\mathbf{Z}/2$. We say that decomposition type of $p(X)$ mod 2 is $1, 3$. Therefore, either p is irreducible over $\mathbf{Z}$ or if not, it is a product of a linear factor and an irreducible factor of degree 3 over $\mathbf{Z}$. But, modulo 11, we have $p(X) = (X^2 + 5X - 1)(X^2 - 5X - 4)$ where both factors are irreducible over the field $\mathbf{Z}/11$. That is, the decomposition type of p mod 11 is $2, 2$. Thus, it cannot be that p has a linear factor over $\mathbf{Z}$. In other words, p must be irreducible over $\mathbf{Z}$.

(Eisenstein's criterion)
If A is a domain and $0 \neq f = \sum_{i=0}^{n} a_i X^i \in A[X]$ is monic such that there is a prime element $p \in A$ satisfying $p/a_i; 0 \leq i < n$, $p \not| a_n, p^2 \not| a_0$, then f is an irreducible element.
The proof is easy. Indeed, reduce the coefficients of f modulo the prime ideal (p) in A. Thus, we have a homomorphism from $A[X]$ to $(A/(p))[X]$ and let us denote the image of any $a \in A$ in $A/(p)$ by $\bar{a}$ and that of a polynomial $u \in A[X]$ by $\bar{u}$. Now, if $f = gh$ in $A[X]$ with the degrees of g and h less than n, we have $X^n = \bar{g}\bar{h}$. Writing

$$g = g_0 + g_1 X + \cdots + g_r X^r,$$

$$h = h_0 + h_1 X + \cdots + h_s X^s,$$

we have $\bar{g_0}\bar{h_0} = 0$. As $A/(p)$ is a domain, one of these is zero. Exactly one of them only can be zero since p^2 does not divide $a_0 = g_0 h_0$. Suppose $\bar{g_0} = 0 \neq \bar{h_0}$. Then, recursively, comparing the coefficients of X, X^2 etc. in the equation $X^n = \bar{g}\bar{h}$ we obtain $\bar{g_1} = 0 = \bar{g_2}$ etc. Finally, we obtain $\bar{g_r} = 0$ which contradicts the fact that g_r is a unit in A because $g_r h_s = 1$. Therefore,

§ The basis theorem

In this section, we discuss the following basic result due to Hilbert which, together with Hilbert's nullstellensatz, gave birth to modern algebraic geometry. The proof is existential and prompted one top mathematician of those times to remark "das is nicht mathematik; das ist theologie" (this is not mathematics; it is theology).

Hilbert Basis theorem
Let A be a ring in which each ideal is finitely generated. Then, the same holds for $A[X]$.
In particular, ideals in $\mathbf{Z}[X]$ are finitely generated; we already saw that this is not a PID although $\mathbf{Z}$ is.
Proof :
Let $I \subset A[X]$ be any non-zero ideal. We consider the subset J_n of A consisting of zero along with all those elements which occur as the top coefficient of some non-zero polynomial of degree $\leq n$ in $A[X]$. Then, J_n is an ideal of A and, $J_n \subset J_{n+1}$ for each n. Note that if a monic polynomial of some degree n exists in I, then all J_m for $m \geq n$ are unit ideals. Let also $J = \bigcup_{n \geq 0} J_n$. By hypothesis, there are generators $a_1, \cdots, a_r$ of J. Choose and fix $f_1, \cdots, f_r \in A[X]$ which have top coeficients $a_1, \cdots, a_r$. Suppose N is the maximum of the degrees of the f_i's. Now, we consider the ideals $J_0, \cdots, J_{N-1}$. Choose a finite set of generators for each of them and choose corresponding polynomials in I whose top coefficients are these generators. Call the polynomials corresponding to J_k to be $f_{k1}, \cdots, f_{k,t_k}$ for each $k = 0, \cdots, N-1$. We claim that the polynomials $f_1, \cdots, f_r$ along with these polynomials generate I. This will be proved by induction. Let $f \in I$. If deg $f = 0$ then $f \in J_0$ and we are done. Suppose deg $f > 0$. If deg $f \geq N$, then we write a for the top coefficient of f. Then, since $a = \sum_{i=1}^{r} b_i a_i$ for some $b_i \in A$, we have $f - \sum_i b_i X^{degf - degf_i} f_i$ is an element of I with degree $<$ deg f. By the induction hypothesis, we get the assertion for f. Now, if deg $f = n < N$, clearly its top coefficient c is expressible as a A-linear combination of generators of J_n. But then subtracting from f, the same A-linear combination of the elements $f_{n1}, \cdots, f_{n,t_n}$, we have a polynomial in I of smaller degree than f. By the induction hypothesis, we are through.

From the above, we have in $K[X_1, \cdots, X_n]$ for any field K, that ideals are finitely generated. The usefulness of this result is that in $\mathbf{K}^n$, the set of points of intersection of an infinite set of polynomial equations in n variables, is also the set of points of intersection of finitely many polynomials.

Note that if $I \subseteq K[X_1, \cdots, X_n]$ is a nonzero ideal, the above proof involves the set

$$LT(I) := \{cX_1^{i_1} \cdots X_n^{i_n} : \exists f \in I, cX_1^{i_1} \cdots X_n^{i_n} = LT(f)\}$$

where $LT(f)$ denotes the leading term of f. Notice that if $f_1, \cdots, f_r$ generate I, then the ideal generated by $LT(f_i)$, $i = 1, \cdots, n$ is contained in the ideal generated by $LT(I)$.
It may very well happen that these are unequal. For instance, if $f_1 = X^3 - 2XY, f_2 = X^2Y - 2Y^2 + X$ and $I =< f_1, f_2 > \subset K[X, Y]$, then $X^2 \in I$. So, $X^2 \in < LT(I) >$ but it is easy to see that $X^2 \notin < LT(f_1), LT(f_2) >$.
But, in general, it is a fact that one may *choose* generators $f_1, \cdots, f_r$ for any ideal I such that

$$< LT(I) >=< LT(f_1), \cdots, LT(f_r) > .$$

Such a basis is called a Gröbner basis and it has nowadays grown to be a very powerful method of doing constructive algebraic geometry.

Some questions on commutative rings for UGC course Nov. 2003

B.Sury

In what follows, A is a commutative ring containing 1.

Q 1.
Let I be a finitely generated ideal of A in which each element a can be expressed as a finite sum $b_1c_1 + b_2c_2 + \cdots + b_nc_n$ for some $b_i, c_i \in I$ and some $n \geq 1$. Prove that I can be generated by a single element e satisfying $e^2 = e$.

Q 2.
Suppose every ideal in A is finitely generated. Let $\theta : A \to A$ be a ring homomorphism which is onto. Prove that θ must also be $1-1$.

Q 3.
Suppose A is an integral domain. Then prove that A is a UFD if, and only if, every nonzero prime ideal contains a prime element.

Q 4.
Show that if every prime ideal of A is finitely generated, then so is every ideal.
Show that if every prime ideal is principal, then so is every ideal.

Q 5.
Suppose A is a UFD and K denotes its quotient field. If f is a monic integral polynomial, say $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ with $a_i \in A$ and, if $f(a/b) = 0$ for some $a/b \in K$, prove that $a/b \in A$.
Apply this to $A = \mathbb{Z}$ to deduce that $\sqrt{2}$ is irrational.

Q 6.
Find all the ideals of the ring $\mathbb{Z}[X]$.

Q 7.
Prove the following generalisation of Eisenstein's criterion.
Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be an integral polynomial satisfying the following property with respect to some prime p. There exists $0 < t \leq n$ be such that the prime p divides $a_0, a_1, \cdots, a_{n-t}$ but does not divide a_n. Also,

assume that p^2 does not divide a_0. Then, f is either irreducible or it has a nonconstant factor of degree less than t.

Q 8.
Show that the quotient ring $K[X,Y]/(X^2+Y^2-1)$ is a UFD if $K=\mathbb{C}$ and is not a UFD if $K=\mathbb{R}$.

Q 9.
Let $A \subset B$ be domains and assume that each $b \in B$ satisfies a monic polynomial with coefficients in A. Prove that A is a field if, and only if, B is a field.

Q 10.
Let d be any (positive or negative) integer such that $|d| = p_1 p_2 \cdots p_r$ where p_i are distinct primes. If $K = \{a+b\sqrt{d} \in \mathbb{C} : a,b \in \mathbb{Q}\}$, then show that the subset $B := \{z \in K : z$ satisfies a monic integral polynomial $\}$ equals, respectively, $\{a+b\sqrt{d} \in \mathbb{C} : a,b \in \mathbb{Z}\}$, or $\{a+b\frac{1+\sqrt{d}}{2} \in \mathbb{C} : a,b \in \mathbb{Z}\}$ according as whether $d \equiv 2,3$ mod 4 or $d \equiv 1$ mod 4.