Computer Science & Engineering Department
IIT Kharagpur
Computational Number Theory: CS60094
Lecture VIII

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Finite Fields

1.1 Introduction

An *integral domain* is a *commutative ring with identity* where $1 \neq 0$ and $a \times b = 0$ implies that either $a = 0$ or $b = 0$. The set of integers, $\mathbb{Z}$, is an *integeral domain*. A *field* is a *commutative ring with identity* where every non-zero element is invertible. A *finite field* has finite number of elements e.g. $\mathbb{F}_q$ is a field with q elements[1]. It is often called a *Galois field* and $GF(q)$ is also used as a notation. It is known that $(\mathbb{Z}_p, +_p, \times_p, 0, 1)$ is a field if p is prime[2]. This is a *Galois field* $\mathbb{F}_p$ of order p.

Example 1. The set $\mathbb{F}_2 = \{0, 1\}$ under modulo 2 addition and multiplication is a field.
In fact for every positive integer n and every prime p, there is a field with p^n elements. We start with a few definitions.

Let R be a ring with identity. There is a map $\mathbb{Z} \to R$ such that $0 \mapsto 0_R$, the additive identity of R, $1 \mapsto 1_R$, the multiplicative identity of R. If $n > 1$, $n \mapsto n_R = \overbrace{1_R + \cdots + 1_R}^{n}$, and if $n < 0$, then $n \mapsto n_R = -(-n)_R$, where the inner minus is on integer n and the outer minus is for the additive inverse in R. If there is no ambiguity, we shall use n for n_R.
Definition 1: In a ring R, the smallest positive integer n, if it exists, is called the characteristic of R, *char*(R), if $\underbrace{1_R + \cdots + 1_R}_{n} = n \times 1_R = 0$. If there is no such n, then *char*$(R) = 0$.

Example 2. *Char*$(\mathbb{Z}_n) = n$, for a positive integer $n > 1$ and *Char*$(\mathbb{Z}) = 0$
Proposition 1. If D is an *integral domain* where *Char*$(D) > 0$, then *Char*(D) is a prime number. A finite integral domain(field) D has a prime characteristic. QED.

Proof: Let *Char*$(D) = n > 0$ be a composite number, so $n = pq$, where $1 < p, q < n$. But then we have

$$0 = n \times 1 = (pq) \times 1 = \overbrace{1 + \cdots + 1}^{pq} = \overbrace{\overbrace{1 + \cdots + 1}^{p} + \cdots + \overbrace{1 + \cdots + 1}^{p}}^{q} = \overbrace{p_F + \cdots + p_F}^{q}$$

Now $p_D \cdot (\overbrace{1 + \cdots + 1}^{q}) = p_D \cdot q_D$. But an ntegral domain does not a have a zero divisor[3], so either $p_D = 0$ or $q_D = 0$. It contradicts our assumption that $1 < p, q < n$.

In a finite integral domain $1_D, 1_D + 1_D = 2_D, 1_D + 1_D + 1_D = 3_D, \cdots$ cannot be all distinct. So we have $p_D = q_D$, where $p < q$. By cancelling p elements we get $(q - p)_D = 0$. So the characteristic is positive and we already have proved that it is a prime. QED.

A *subfield* F' of a field F is defined in the usual way: $F' \subseteq F$ and F' is a field under the operations of F restricted to F'. It is not difficult to prove that intesection of subfields will form a subfield.

---

[1] We shall prove that all fields with q elements are isomorphic.

[2] $(\mathbb{Z}_p, +_p, \times_p, 0, 1)$ is a *commutative ring with identity*. And for all $a \in \mathbb{Z}_p \setminus \{0\}$, $ax = 1$ has a solution in $\mathbb{Z}_p$ as $ax \equiv 1 (\text{mod } p)$ has a solution.

[3] Let $a, b \in F$ and $a \neq 0 \neq b$, but $ab = 0$. Multiplying both sides by a^{-1} we get $b = 0$, a contradiction.

Let F be a field, it has the *smallest subfield*, the intersection of all subfields of F. It is known as *prime subfield* of F.

If F and F' are two fields, then a map $\phi : F \to F'$ is called a *field homomorphism* if $\phi(a +_F b) = \phi(a) +_{F'} \phi(b)$ and $\phi(a \times_F b) = \phi(a) \times_{F'} \phi(b)$.

Example 3. Let F and F' be two fields and the map $\phi : F \to F'$ be a homomorphism. Following facts can be verified.

1. $\phi(0_F) = 0_{F'}$: $\phi(0_F) = \phi(0_F + 0_F) = \phi(0_F) +_{F'} \phi(0_F)$. So $\phi(0_F) = 0_{F'}$.
2. $\phi(1_F) = 1_{F'}$: the justification is similar.
3. $-\phi(a) = \phi(-a)$: $0_{F'} = \phi(0_F) = \phi(a +_F (-a)) = \phi(a) +_{F'} \phi(-a)$. So $-\phi(a) = \phi(-a)$.
4. $\phi(a)^{-1} = \phi(a^{-1})$: the justification is similar.
5. $Im(\phi)$ or $\phi(F)$ is a subfield of F': let $\phi(a), \phi(b) \in F'$ for some $a, b \in F$. We know that $\phi(a) +_{F'} \phi(b) = \phi(a +_F b) \in \phi(F)$. Similarly it is possible to show that $\phi(a) \times_{F'} \phi(b) \in \phi(F)$. So $\phi(F)$ is closed under both the operations. We have already seen that the identity elements of both the operations are in $\phi(F)$, and if $\phi(a) \in \phi(F)$, then its inverse is also there. Associative and distributive laws are satisfied.
6. Let $F'' \subseteq F'$ be a subfield of F'. $\phi^{-1}(F'') = \{a \in F : \exists b \in F'', \phi(a) = b\}$ is a subfield of F: as $0_{F'} = \phi(0_F)$ and $1_{F'} = \phi(1_F)$ are in F'', $0_F, 1_F \in \phi^{-1}(F'')$.
   If $a \in \phi^{-1}(F'')$, then $\phi(a) \in F''$. So, $\phi(a)^{-1} \in F''$. But we know that $\phi(a^{-1}) = \phi(a)^{-1}$, so $a^{-1} \in \phi^{-1}(F'')$.
   Finally if $a, b \in \phi^{-1}(F'')$, $\phi(a), \phi(b) \in F''$ and both $\phi(a) +_{F'} \phi(b) = \phi(a +_F b)$ and $\phi(a) \times_{F'} \phi(b) = \phi(a \times_{F'} b)$ are in $\phi^{-1}(F'')$. So $a +_F b$ and $a \times_{F'} b$ are in $\phi^{-1}(F'')$.

Proposition 2. If F is a finite field so that $char(F) = p$, then the *prime subfield* of F is *isomorphic* to $\mathbb{F}_p$. QED.

Proof: We define a map $\phi : \mathbb{F}_p \to F$ so that $n \mapsto \overbrace{1 + \cdots + 1}^{n}$. We observe that

$$\phi(m+n) = \overbrace{1 + \cdots + 1}^{m+n} = \overbrace{1 + \cdots + 1}^{m} + \overbrace{1 + \cdots + 1}^{n} = \phi(m) + \phi(n),$$

and also

$$\begin{aligned} & \phi(mn) \\ = & \overbrace{1 + \cdots + 1}^{mn} \\ = & \overbrace{\overbrace{1 + \cdots + 1}^{n} + \cdots + \overbrace{1 + \cdots + 1}^{n}}^{m} \\ = & \overbrace{\phi(n) + \cdots + \phi(n)}^{m} \\ = & \phi(n)(\overbrace{1 + \cdots + 1}) \\ = & \phi(n) \cdot \phi(m). \end{aligned}$$

So the map ϕ is a homomorphism. We further show that ϕ is an injection i.e. a monomorphism.

Assume that $\phi(a) = \phi(b)$, where $0 \le a < b < p$. Then we have $c = b - a > 0$.

$$\begin{aligned} \phi(1) &= \phi(c \cdot c^{-1}) = \phi(c) \cdot \phi(c^{-1}) \\ &= \phi(b-a) \cdot \phi(c^{-1}) \\ &= (\phi(b) + (-\phi(a))) \cdot \phi(c^{-1}) \\ &= 0_F \cdot \phi(c^{-1}) = 0_F. \end{aligned}$$

But $\phi(1) = 1_F \ne 0_F$ - a contradiction. ϕ is an injection and the image of $\mathbb{F}_p$ in F, $\phi(\mathbb{F}_p)$ is a subfield of F.

It is known that $\mathbb{F}_p$ does not have any proper subfield and is its own *prime*. So $\phi(\mathbb{F}_p)$, is the smallest or *prime* subfield of F which can be identified with $\mathbb{F}p$. QED.

1.2 Vector Space

We have not seen so far any finite field other than $\mathbb{F}_p$. We introduce the concept of *vector space* and claim that a field F is a vector space over its subfield.
The concept of vector space is a generalisation of the collection of Euclidean vectors over $\mathbb{R}^n$. Following is the formal definition.
Definition 2: A *vector space* over a field F is a set V equipped with the binary opeartion "addition" defined on its elements and multiplication by the elements of F (known as scalar), satisfying the following set of axioms:

1. V is a *commutative* group under vector addition.
2. The scalar multiplication is distributed over vector addition, i.e. for all $u, v \in V$ and for all $a \in F$, $a(u + v) = au + av$.
3. The vector multiplication is distributed over scalar addition, i.e. for all $u \in V$ and for all $a, b \in F$, $(a + b)u = au + av$.
4. For all $u \in V$ and for all $a, b \in F$, $(ab)u = a(bu)$.
5. For all $u \in V$, $1u = u$.

Elements of a vector space are called *vectors*. The identity element of vector addition is known as the *null vector* 0.

Example 4. Following are a few examples of vector spaces.

1. 2, 3, or n dimensional Euclidean vector spaces over $\mathbb{R}$. The addition of two vectors and multiplication by scalar are as usual.
2. Given any field F and a positive integer n, the collection of n-tuples of elements of F, F^n, is a vector space over F under the following definition of addition and scalar multiplication:
   Let $(a_1, \cdots, a_n), (b_1, \cdots, b_n) \in F^n$ and $c \in F$.
   - $(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n)$, and
   - $c(a_1, \cdots, a_n) = (ca_1, \cdots, ca_n)$.

   By this definition $\mathbb{C}$ is a vector space over $\mathbb{R}$.
3. The collection of all functions from a non-empty set A to F, where F is a field, is a vector space over F where addition and scalar multiplication are defined as follows:
   Let $f, g \in F^A$ and $c \in F$.
   - $(f + g)(a) = f(a) + g(a)$, for all $a \in A$, and
   - $(cf)(a) = c(f(a))$, for all $a \in A$.
4. All 2×2 matrices over $\mathbb{R}$, $\mathcal{M}_2(\mathbb{R})$, is a vector space.
5. If L be a subfield of F, then F may be viewed as a vector space over L in a natural way under the addition and multiplication of the field F.

Definition 3: Let V be a *vector space* over the field F and $U \subseteq V$. The subset U is called a *subspace* of V if it satisfies the following conditions:

1. U is a subgroup of V,
2. if $u \in U$, then for all $a \in F$, $au \in U$.

Example 5. In $\mathbb{R}^3$, vectors lying on a plane passing through the origin forms a subspace of $\mathbb{R}^3$. Similarly vectors along a line passing through origin also forms a subspace of $\mathbb{R}^3$. Finally the *null vector* $(0,0,0)^T$ (origin) alone forms a subspace.

In connection to the Euclidean space $\mathbb{R}^3$, we know that there are three *unit vectors* $u = (1,0,0)^T, v = (0,1,0)^T, w = (0,0,1)^T$. Any vector $a \in \mathbb{R}^3$ can be expressed as a linear combination of the unit vectors, $a = (x,y,z)^T = xu + yv + zw$, where $x, y, z \in \mathbb{R}$, are known as the coordinates of a. The set $\{u, v, w\}$ is called a *basis* of the vector space $\mathbb{R}^3$.
We also know that the *basis* set is not unique and any set of three non-coplanar vectors can form a *basis* for $\mathbb{R}^3$. In general we have the following definitions.
Definition 4: Let V be a vector space over a field F and let $u_1, \cdots, u_n \in V$. A *linear combination* of these n vectors is $a_1u_1 + \cdots + a_nu_n$, where $a_1, \cdots, a_n \in F$. The linear combination is called *trivial* if $a_1 = \cdots = a_n = 0 \in F$; otherwise it is called *nontrivial*.
Let $U = \{u_1, \cdots, u_n\} \subseteq V$. U is called *linearly dependent* if there is a *nontrivial linear combination* that gives the *null vector* (0). Otherwise the set is called *linearly independent*.

Example 6. In $\mathbb{R}^3$, $u_1 = (-1,-3,-1)^T$, $u_2 = (2,-2,-2)^T$, $u_3 = (-4,0,2)^T$ are *linearly dependent* as

$$2(-1,-3,-1)^T + (-3)(2,-2,-2)^T + (-2)(-4,0,2)^T = (0,0,0).$$

But, $(1,2,-1)^T$, $(1,-1,2)^T$ and $(-1,3,-1)$ are *linearly independent*. We can show this by proving that $x(1,2,-1)^T + y(1,-1,2)^T + z((-1,3,-1)) = (0,0,0)^T$ does not have any solution other than $(0,0,0)$.
Proposition 3. Let V be a vector space over the field F. The vectors $u_1, \cdots, u_n \in V$ are *linearly dependent* if and only if one of them is a non-trivial linear combination of the other. QED.

Proof: Without any loss of generality we assume that $u_1 = a_2u_2 + \cdots + a_nu_n$. So we have $u_1 - a_2u_2 - \cdots - a_nu_n = 0$, a *non-trivial* linear combination $\{u_1, \cdots, u_n\}$ gives the *null* vector.
In the other direction we assume that $a_1u_1 + \cdots + a_nu_n = 0$. One of $a_i \neq 0$. So we have $u_i = \frac{-a_1}{a_i}u_1 + \cdots + \frac{-a_{i-1}}{a_i}u_{i-1} + \frac{-a_{i+1}}{a_i}u_{i+1} + \cdots + \frac{-a_n}{a_i}u_n$. QED.
A set U of vectors is *linearly dependent* does not mean that every element of U can be expressed as a linear combination of the other.

Example 7. Consider $u_1 = (1,2,3)^T$, $u_2 = (2,4,6)^T$ and $u_3 = (1,1,1)$. They are *linearly dependent* as $2u_1 - u_2 = 0$. But u_3 cannot be expressed as linear combination of u_1 and u_2 as they are along the same line, but the line of support of u_3 is different.
Definition 5: Let V be a vector space over the field F and $S \subseteq V$. The *linear span* of S, denoted by $< S >$, is defined as follows:

$$< S >= \left\{ \sum_{i=1}^{n} a_iu_i : \ n \in \mathbb{N}, \ a_i \in F, \ u_i \in S \right\}.$$

Definition 6: A vector space V over a field F is said to be *finite dimensional* if there is a finite subset S of V so that $< S >= V$. Otherwise it is infinite dimensional.

Example 8. We consider $\mathbb{R}[X]$, the polynomial functions of single variable on the real field. It is not difficult to check that $\mathbb{R}[X]$ is a vector space over $\mathbb{R}$. But this space cannot be spanned by any finite set. One set that spans this space is $S = \{x^n : n = 0, 1, 2, \cdots\}$. The set S may be viewed as a collection of e_i's, $i \in \mathbb{N}$, where $e_i = (a_i)_{i=1}^{\infty}$ such that $a_j = 1$ if $i = j$ but $a_j = 0$ if $i \neq j$. Any polynomial can be written as a linear combination of finite number of elements of S. So it is an infinite dimentional vector space.
Definition 7: Let V be a finite dimensional vector space over the field F. A set $B = \{e_1, \cdots, e_n\} \subset V$ is called a *basis* of V if the vectors of B are *linearly independent* and $< B >= V$.

It can be proved that every vector space finite or infinite dimensionsl has a *basis*. The proof requirs *Zorn's lemma*[4], a variation of *Axiom of Choice*[5]. The basis may be uncountably infinite.

Example 9. Consider the vector space $\mathbb{R}^\infty = \{(a_i)_{i=1}^\infty : a_i \in \mathbb{R}\}$. It cannot have a *countable basis*(why?).

Proposition 4. If a vector space V over the field F is spanned by m vectors, then any set of n vectors of V, where $n > m$, are *linearly dependent*. QED.

Proof: Let $V =< \{u_1, \cdots, u_m\} >$ and $v_1, \cdots, v_n \in V$. So we have

$$\begin{aligned} v_1 &= a_{11}u_1 + \cdots + a_{1m}u_m \\ \vdots & \vdots \ \vdots \\ v_n &= a_{n1}u_1 + \cdots + a_{nm}u_m \end{aligned}$$

We consider the following system of m homogeneous equations:

$$\begin{aligned} a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n &= 0 \\ \vdots & \vdots \ \vdots \\ a_{1m}x_1 + a_{2m}x_2 + \cdots + a_{nm}x_n &= 0 \end{aligned}$$

The number of unknowns n in these equations is greater than the number of equations m It is known that there is a *non-null* solution of this system. Let the solution be $(b_1, \cdots, b_n)$.
So we have

$$\begin{aligned} b_1v_1 + \cdots + b_nv_n &= b_1(a_{11}u_1 + \cdots + a_{1m}u_m) + \cdots + b_n(a_{n1}u_1 + \cdots + a_{nm}u_m) \\ &= u_1(a_{11}b_1 + \cdots + a_{n1}b_n) + \cdots + u_m(a_{1m}b_1 + \cdots + a_{nm}b_n) \\ &= 0. \end{aligned}$$

So $v_1, \cdots, v_n$ are linearly dependent. QED.

Proposition 5. All bases of a finite-dimensional vector space V over a field F contains same number of vectors. QED.

Proof: Let B_1 and B_2 be two bases of V with n_1 and n_2 vectors so that $n_2 > n_1$. But according to the previous proposition n_2 vectors of B_2 are linearly dependent. This is contradictory. QED.

The size of a *basis* of a finite-dimensional vector space is known as *dimension* of the vector space, *dim* V.

We use the concept of vector space to characterise the size of a finite field. We know that a field F may be viewed as a vector space of its subfield K. Let *char*$(F) = p$, a prime, and $|F| > p$. We know that $\mathbb{F}p$ is isomorphic to the *prime subfield* of F. So F may be viewed as a vector space over $\mathbb{F}p$. Let the dimension of F over $\mathbb{F}_p$ or the *degree* or $[F : \mathbb{F}p]$ be n. We have the following proposition.

Proposition 6. If F is a finite field with *char*$(F) = p$, then there is a positive integer n such that $|F| = p^n$. QED.

Proof: We know that $[F : \mathbb{F}p] = n$. So a basis of F is an n element subset $B = \{u_1, \cdots, u_n\}$ of F. Every element of $v \in F$ can be expressed as a linear combination $a_1u_1 + \cdots + a_nu_n = v$, where $a_i \in \mathbb{F}p$. There are p elements in $\mathbb{F}p$, so we have p^n linear combinations[6]. So there are p^n elements in F. QED.

[4] Zorn's lemma is also known as Kuratowski-Zorn lemma. Let P be a collection of subsets of some set A. P has the property that whenever there is a chain of subsets $A_1 \subset A_2 \subset \cdots$ in P, then their union $\cup A_i$ is in P. According to *Zorn's lemma*, P has a *maximal element* A_m i.e. there is no $B \in P$ such that $A_m \subset B$.

[5] There are different versions of this axiom of set theory. It assumes that for evey indexed family of non-empty sets $\{A_i\}_{i\in I}$, there is an indexed family of elements $\{a_i\}_{i\in I}$ such that $a_i \in A_i$ for all $i \in I$.

[6] Two linear combinations cannot give the same element of F. If $a_1u_1 + \cdots + a_nu_n = b_1u_1 + \cdots + b_nu_n$, then $(a_1 - b_1)u_1 + \cdots + (a_n - b_n)u_n = 0$. But that is impossible as $u_1, \cdots, u_n$ are linearly independent.

So the number of elements of any finite field can be a power of some prime.

Example 10. We consider the case of $\mathbb{F}_{2^2}$. We know that $\mathbb{F}_2$ is embedded in $\mathbb{F}_{2^2}$. So we take 0 and 1 with their usual meaning. Let a be another element, so $a+1$ is the fourth element to make the set closed under addition. We know that $char(\mathbb{F}_{2^2}) = 2$ i.e. $1+1=0$, then for all $x \in \mathbb{F}_{2^2}$, $x+x=0$. We also cannot have $a \cdot a = a$ or $a(a+1) = a+1$, as that implies $a=1$. $a(a+1)=a$ implies that $a=0$. So we have the following addition and multiplication tables.

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\times$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

What can be a basis for $\mathbb{F}_{2^2}$? Clearly 0 cannot be there in the basis as $\{0, u\}$ is always linearly dependent: $c \cdot 0 + 0 \cdot u = 0$, where $c \neq 0$. We may have $\{1, a\}$.

For a prime p, $GF(p)$, $\mathbb{Z}_p$ and $\mathbb{F}_p$ means the same field. But if $n = p^k$, where p is a prime and $k > 1$, then $\mathbb{Z}_n$ is algebraically different from $GF(n)$ or $\mathbb{F}_n$, where $\mathbb{Z}_n$ is not a field, has $p^k - (\phi(p^k)+1) = p^k - p^k + p^{k-1} - 1 = p^{k-1} - 1$ *zero divisors*.

Example 11. In $\mathbb{Z}_4$ we have $2 \times_4 2 = 0$. But the multiplication table of $\mathbb{F}4$ does not have any such element. have any such

1.3 Polynomials

A *polynomial* over a *ring* R is a function $f : R \to R$ of the form $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_i x + \cdots + a_n x^n$, where $a_i \in R$.
If all a_i's are 0, then it is called a *zero polynomial*, and is denoted by 0. If the *leading coefficient* $a_n \neq 0$, then n is called the *degree* of f, denoted by $deg(f)$. By convention the degree of the *zero polynomial* is $-\infty$. A polynomial f is called a *constant polynomial* if $dig(f)$ is 0 or $-\infty$. If the ring R has the multiplicative *identity element* 1, and $a_n = 1$, then $f(x)$ is called a *monic polynomial*.
Two polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ are said to be equal if and only if $a_i = b_i$ for all $i = 0, \cdots, n$.
Polynomial f and g can be added to get $h(x) = \sum_{i=0}^{n} c_i x^i$, where $c_i = a_i + b_i$ for all $i = 0, \cdots, n$. We can pad a polynomial with zero coefficients for the purpose of comparison and addition. But normally *terms* with zero coefficients are not written explicitly.

Example 12. Let $f(x) = 2x^2 - 5$ and $g(x) = 7x^3 + 5x + 6$. The sum $h(x) = f(x) + g(x) = (0+7)x^3 + (2+0)x^2 + (0+5)x + (-5+6) = 7x^3 + 2x^2 + 5x + 1$.

Product of two polynomials, $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ is

$$h(x) = f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k, \text{ where } c_k = \sum_{0 \le i \le n \wedge 0 \le j \le m}^{i+j=k} a_i b_j.$$

Example 13. Let $f(x) = 2x^2 - 5x$ and $g(x) = 7x^3 + 2x^2 + 6$. The product $h(x) = (2 \times 7)x^5 + (2 \times 2 + 7 \times (-5))x^4 + (-5 \times 2)x^3 + (2 \times 6)x^2 + (-5 \times 6)x = 14x^5 - 31x^4 - 10x^3 + 12x^2 - 30x$.

Given the above definitions, it is clear that collection of all polynomials over R, denoted by $R[x]$, forms a ring.

Example 14. Let $R = \mathbb{Z}_6$ and $f(x) = 2x^2 + 1$ and $g(x) = 4x^2 + 3x$. So $f(x) + g(x) = (2+4)x^2 + 3x + 1 = 3x + 1$.
If we take $h(x) = 3x^2$, then $f(x)h(x) = 3x^2$. Finally if we take $k(x) = 2x^2$, then $h(x)k(x) = 0$, the product of two non-zero polynomial is a zero polynomial. So it is not an *integral domain*.
We have $deg(f+g) \le max(deg(f)\ deg(g))$, and $deg(fg) \le deg(f) + deg(g)$.

$R[x]$, the ring of polynomials over R, is commutative, if R is commutative. $R[x]$ has the identity element 1 if R is a ring with identity. We are interested about polynomials over a *field*, where every non-zero element is invertible and there is no *zero-divisor*.

Let F be a *field*. Polynomial division over $F[x]$ is similar to integer division. The division algorithm is as follows:
If $g, f \in F[x]$ are such that $g \neq 0$, then there exists $q, r \in F[x]$, such that $f(x) = g(x)q(x) + r(x)$, where $deg(r) < deg(g)$. *The polynomial g divides the polynomial f if $r = 0$ i.e. $f = gq$.*

Example 15. Let the field be $\mathbb{F}_7$ and $g(x) = 3x^2 + 2$, $f(x) = 2x^5 + 4x^3 + 3x + 1$ be polynomials over $\mathbb{F}_7$. We do the usual long division.
The first term of the quotient is $3x^3$ as $3x^2 \times 3x^3 = 2x^5$. The first partial remainder is $r_1(x)$,

$$\begin{aligned} r_1(x) &= f(x) - 3x^3(3x^2 + 2) \\ &= 2x^5 + 4x^3 + 3x + 1 - (2x^5 + 6x^3) \\ &= 2x^5 + 4x^3 + 3x + 1 + (-2)x^5 + (-6)x^3 \\ &= 5x^3 + 3x + 1. \end{aligned}$$

The second term of the quotient is $4x$ as $4x \times 3x^2 = 5x^3$. The final remainder is $r(x)$,

$$\begin{aligned} r(x) &= r_1(x) - 4x(3x^2 + 2) \\ &= 5x^3 + 3x + 1 - (5x^3 + x) \\ &= 5x^3 + 3x + 1 + (-5)x^3 + (-1)x \\ &= 2x + 1. \end{aligned}$$

So we have

$$2x^5 + 4x^3 + 3x + 1 = (3x^2 + 2)(3x^3 + 4x) + (2x + 1).$$

Given a ring R and $S \subseteq R$, S is a subring of R, if S is an additive subgroup and is closed under multiplication. If the ring has an identity element 1, the conditions for S to be a subring are (i) $-1 \in S$, (ii) S is closed under addition, and (iii) S is closed under multiplication[7]*. A subring I of R is an ideal, if for all $a \in I$ and all $r \in R$, ar and $ra \in I$. We also know that for a commutative ring R with identity, the smallest ideal that contains $a \in R$ is $(a) = \{ar : r \in R\}$. This is called the principal ideal generated by a.*

Example 16. Consider $\mathbb{Z}$ the ring of integers. Take $105 \in \mathbb{Z}$. The ideals that contain 105 are $\{\cdots, -6, -3, 0, 3, 6, \cdots\}$, $\{\cdots, -10, -5, 0, 5, 10, \cdots\}$ and $\{\cdots, -14, -7, 0, 7, 14, \cdots\}$, $\mathbb{Z}$.
But the smallest one is $(105) = \{\cdots, -210, -105, 0, 105, 210, \cdots\}$, the principal ideal generated by 105.

Definition 8: An integral domain D where every ideal is a principle ideal is called a principle ideal domain (PID).

Example 17. $\mathbb{Z}$ is a PID where every ideal is of the form $n\mathbb{Z}$, $n \in \mathbb{Z}$.

An ideal I over the ring R defines a partition as it is a subgroup (normal) under addition. The equivalence classes are called residue classes modulo I and are cosets of I. For each element $a \in R$, an equivalence class $[a] = a + I$. Two elements $b, c \in R$ are equivalent modulo I if they belong to the same equivalence class say $[a]$ i.e. $b = a + p$ and $c = a + q$, where $p, q \in I$. This implies that $b - c = p - q \in I$[8]*. It is denoted as $b \equiv c(\text{mod } I)$. The equivalence classes modulo n over $\mathbb{Z}$ are essentially equivalences classes modulo the ideal $n\mathbb{Z}$.*

We can naturally define addition and multiplication operations on the quotient set: $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$. So the quotient set is also a ring called quotient ring R/I.

[7] Let $a \in R$, then $(-1)a = -a \in R$ and $a + (-1)a = a - a = 0 \in R$. For a finite ring, closure under addition and multiplication is enough to form a subring.
[8] In multiplicative notation $bc^{-1} \in I$.

On $\mathbb{Z}$ the quotient ring (commutative with identity) modulo n is $\mathbb{Z}/n\mathbb{Z}$ but we also use the old notation $\mathbb{Z}_n$

Proposition 7. *If F is a field, then $F[x]$ is a principal ideal domain. For every ideal I, either $I = (0)$ or there is a unique monic polynomial $f \in F[x]$ such that I is generated by f.* QED.

Proof: *We have (0), the zero-polynomial.*
If $I \neq \{0\}$, then there is a non-zero polynomial $h(x)$ of minimal degree in I. If $h(x)$ is monic, then we take $f(x) = h(x)$, otherwise we take $f(x) = a^{-1}h(x)$, where a is the leading coefficient of $h(x)$. So f is monic and is in I.
Let $g \in I$, by division algorithm we have $q, r \in F[x]$ such that $g = fq + r$, where $\deg(r) < \deg(f)$. But then $r = g - fq$, implies that $r \in I$, which is a contradiction. So $r = 0$ and $f|g$ i.e. $(f) = I$.
To prove the uniqueness we assume that $I = (f')$ where $f' \in I$ and is monic. So we have $f = pf' = p(p'f) = (pp')f$ i.e. $pp' = 1$. So both p and p' are constant polynomials. But both f and f' are monic, so $p = 1 = p'$, implies that $f = f'$.
QED.

We define GCD of two polynomials over a field F. Let $f, g \in F[x]$ such that both are not equal to 0. There is a unique monic polynomial d such that (i) d divides both f and g, (ii) any polynomial $c \in F[x]$, dividing both f and g, divides d. We also have the Bezout's identity, $d = uf + vg$, where $u, v \in F[x]$.

Example 18. *Consider $f(x) = 4x^7 + 2x^6 + 3x^4 + 4x^2 + 2x + 2$ and $g(x) = x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 3$ over $\mathbb{F}_5$. We want to compute $\gcd(f, g) = d$ (say). We rewrite $f(x) = 4f'(x)$, where $f'(x) = x^7 + 3x^6 + 2x^4 + x^2 + 3x + 3$. As d is a monic polynomial, the $\gcd(f, g) = \gcd(f', g)$. We divide f' by g and get*

$$\begin{aligned} f'(x) &= g(x)(x) + r_1(x), \text{ where} \\ r_1(x) &= 4x^5 + x^4 + 3x^3 + x^2 + 3 = 4r_1'(x), \text{ where} \\ r_1'(x) &= x^5 + 4x^4 + 2x^3 + 4x^2 + 2. \end{aligned}$$

In the second stage,

$$\begin{aligned} g(x) &= r_1'(x)(x + 4) + r_2(x), \text{ where} \\ r_2(x) &= 3x^4 + 4x^3 + x^2 + 3x = 3r_2'(x), \text{ where} \\ r_2'(x) &= x^4 + 3x^3 + 2x^2 + x. \end{aligned}$$

In the third stage

$$\begin{aligned} r_1'(x) &= r_2'(x)(x + 1) + r_3(x), \text{ where} \\ r_3(x) &= 2x^3 + x^2 + 4x + 2 = 2r_3'(x), \text{ where} \\ r_3'(x) &= x^3 + 3x^2 + 2x + 1. \end{aligned}$$

Finally, $r_3'(x)|r_2'(x)$, so the $\gcd(f, g) = x^3 + 3x^2 + 2x + 1$, and we have

$$\begin{aligned} \gcd(f, g) &= x^3 + 3x^2 + 2x + 1 \\ &= r_3'(x) \\ &= 3r_3(x), \text{ as } (2)^{-1} = 3 \in \mathbb{F}_5, \\ &= 3(r_1'(x) - r_2'(x)(x + 1)) \\ &= 3(r_1'(x) - 2(g(x) - r_1'(x)(x + 4))(x + 1)), \text{ as } r_2'(x) = 2r_2 \\ &= 4(x + 1)g(x) + r_1'(x)(3 + (x + 1)(x + 4)). \\ &= 4(x + 1)g(x) + 4(f'(x) - xg(x))(3 + (x + 1)(x + 4)), \text{ as } r_1'(x) = 4r_1(x) \\ &= (x^2 + 2)f(x) + (x^3 + x + 4)g(x), \text{ as } f'(x) = 4f(x). \end{aligned}$$

So the Bezout's coefficients are, $x^2 + 2$ and $x^3 + x + 4$.
Definition 9: *A polynomial p of positive degree in $F[x]$, where F is a field, is called irreducible in F, if whenever $p = qr$ and $q, r \in F[x]$, then either q or r is a constant polynomial.*
An irreducible polynomial p is also known as prime in $F[x]$.
It is important to mention the field while calling a polynomial irreducible.

Example 19. The polynomial x^2+1 is irreducible in $\mathbb{R}[x]$, but can be factorised as $(x+i)(x-i)$ in $\mathbb{C}[x]$. Similarly x^2-2 is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$. The polynomial x^3+x+1 is irreducible in $\mathbb{F}_2$.

We accept the following facts about polynomials over $F[x]$, where F is a field, without proof.

1. If $f \in F[x]$ is of positive degree, then $f = cp_1^{e_1}\cdots p_k^{e_k}$, where $p_1, \cdots, p_k \in F[x]$ are irreducible polynomials over F and $c \in F$. Compare it with the prime factorisation of integers larger than 1.

2. If an irreducible polynomial p in F divides $f_1 \times \cdots \times f_n$, a product of polynomials in $F[x]$, then one f_i, $1 \leq i \leq n$ is divisible by p. Compare it with the fact that when a prime $p|mn$, then either $p|m$ or $p|n$.

Proposition 8. *The quotient ring $F[x]/(f)$ is a field if and only if f is irreducible in field F.* QED.

Proof: It is clear that the ring is commutative and it has the multiplicative identity element $[1] = 1+(f)$. So this is a field if all non-zero elements are invertible and it does not degenerate i.e. $[0] \neq [1]$.
$(\Leftarrow)$: f is irreducible.
Let $[k] \neq [0]$ in $F[x]/(f)$. As $[k] \neq [0]$, k is not divisible by f. So gcd$(k,f)=1$ and by the Bezout's identity, there are polynomials $u, v \in F[x]/(f)$ such that $uf+vk=1$. As $uf \in (f) = [0]$, we have $[v][k] = [vk] = [1]$. So $[v]$ is inverse of $[k]$.
$(\Rightarrow)$: f is reducible.
If f is a constant polynomial, there are two possibilities,
(i) $f=0$, in that case $F[x]/(0)$ is isomorphic to $F[x]$ as for all $g \in F[x]$, $g+(0)$ is identified with g itself.
(ii) $f = c \neq 0$, in that case $F[x]/(c)$ has only one element as $(c) = \{cg(x) : g(x) \in F[x]\}$ and for each $g(x) \in F[x]$, $cc^{-1}g(x) = g(x)$.
In none of there cases $F[x]/(f)$ is a field.
If $f = gh$, where g, h are not constants and deg(g), deg(h) are less than deg(f). So f does not divide either g or h implies that $[g]$ or $[h]$ are not equal to $[0]$. But $[g][h] = [gh] = [f] = [0]$. So $F[x]/(f)$ has zero divisors and it is not a field. QED.

Compare the proposition with $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$, which is a field $\mathbb{F}_p$ when p is a prime. Now we shall look at the last result more closely. Let $f \in F[x]$ and $f \neq 0$. The ring of residue classes modulo (f) is $F[x]/(f)$, where $(f) = \{f(x)h(x) : h(x) \in F[x]\}$. A residue class $[g] = g+(f)$. Equality of two residue classes is defined as usual: $[g]=[h]$, if $g+(f) = h+(f)$ i.e $g(x)+f(x)f_1(x) = h(x)+f(x)f_2(x)$, for some $f_1(x), f_2(x) \in R[x]$. So, $f|(g-h)$ i.e. $g \equiv h (\text{mod } f)$.
Each residue class $[g]$ has a representative $r \in [g]$ so that $g \equiv r(\text{mod } f)$ and deg$(r) <$ deg(f). It is clear that r is the remainder when g is divided by f i.e. $g = fq+r$. If there is another r' satisfying $g \equiv r'(\text{mod } f)$ and deg$(r') <$ deg(f), then $r \equiv r'(\text{mod } f)$ i.e. $f|(r-r')$, but that is impossible unless $r = r'$. This gives us the distinct representative r of an equivalence class of $F[x]/(f)$. So an equivalence class is of the form $r+(f)$, where $r \in F[x]$ and deg$(r) <$ deg(f). Compare it with the equivalence classes of $\mathbb{Z}$ modulo n, $[0], \cdots, [n-1]$.

In particular if we take $F = \mathbb{F}_p$ and deg$(f) = n$, then the number of polynomials of degree $\leq (n-1)$ are p^n as every coefficient of $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ can take p possible values. So the number of elements of $\mathbb{F}_p[x]/(f)$ is p^n, and this is a filed.

We already know that any finite field can be of size p^n and here is a field of size p^n. So there is a connection. But the question is whether there is an irreducible polynomial of degree n for every positive integer n? How do we get an irreducible polynomial of a certain degree if it exists? For finite field and lower degree we may enumerate.

Example 20. Let us find out the irreducible polynomials of degree 3 over $\mathbb{F}_2$. Any polynomial of degree 3 is of the form $x^3 + a_2x^2 + a_1x + a_0$, where $a_0, a_1, a_2 \in \{0, 1\}$. So there are 8 possibilities. Again any reducible polynomial of degree

3 is of the form $(x+b)(x^2+b_1x+b_0)$ where $b, b_1, b_0 \in \{0,1\}$. Following table computes them.

b	b_1	b_0	$(x+b)(x^2+b_1x+b_0)$
0	0	0	x^3
0	0	1	x^3+x
0	1	0	x^3+x^2
0	1	1	x^3+x^2+x
1	0	0	same
1	0	1	x^3+x^2+x+1
1	1	0	same
1	1	1	x^3+1

So there are two irreducible polynomials of degree 3 over $\mathbb{F}_2$. They are x^3+x^2+1 and x^3+x+1.

Example 21. *The equivalence classes of $\mathbb{F}_2[x]/(f)$, where $f = x^3+x^2+1$, are $[0] = 0+(f)$, $[1] = 1+(f)$, $[x] = x+(f)$, $[x+1] = x+1+(f)$, $[x^2] = x^2+(f)$, $[x^2+1] = x^2+1+(f)$, $[x^2+x] = x^2+x+(f)$, $[x^2+x+1] = x^2+x+1+(f)$.*

The addition and multiplication tables can be constructed following usual rules e.g.
(i) $[x^2]+[x^2+x+1] = (x^2+(f))+(x^2+x+1+(f)) = x+1+(f) = [x+1]$.
(ii) $[x^2]\times[x^2+x+1] = (x^2+(f))\times(x^2+x+1+(f)) = x^2+x+(f) = [x^2+x]$.
The reason for the last one is $x^4+x^3+x^2 = xf(x)+x^2+x$.

Example 22. *We take a simpler example. Take the irreducible polynomial $f(x) = x^2+x+1$ over $\mathbb{F}_2$ of degree-2. The elements of the quotient field are $[0] = 0+(f)$, $[1] = 1+(f)$, $[x] = x+(f)$, and $[x+1] = x+1+(f)$. The addition and multiplication tables are as follows:*

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

As an example,

$$[x]\times[x+1] = (x+(f))(x+1+(f)) = x^2+x+(f) = 1+(f) = [1].$$

The table is same as what we constructed earlier.

1.4 Extension Field

We know that given a field F, a subset K of F is called a subfield of F, if K is a field under the operations of F. If $K \neq F$, then K is a proper subfield of F. The field F is known as an extension of K and is denoted by F/K. A field is called a prime field if it does not have any proper subfield. We already know that for each prime p, $\mathbb{F}_p$ is a prime field.
Definition 10: *Let K be a subfield of F and $M \subseteq F$. The smallest subfield of F containing both M and K is the extension field of K obtained by adjoining M. It is denoted by $K(M)$. If $M = \{\alpha\}$, then we write $K(\alpha)$ and it is called a simple extension of K, where α is known as the defining element of $K(\alpha)$ over K.*

Viewing F as a vector space over K, the dimension of F is denoted by $[F:K]$. It is called the degree of extension. If the degree of extension or the dimension of F over K is finite, then it is called a finite extension.
If an element $\alpha \in F$ is a root of a polynomial equation $a_0+a_1x+\cdots+a_nx^n = 0$, where $a_i \in K$ and not all a_i's are zeros, then we say that α is algebraic over K. An extension L of K is called algebraic over K, if all elements of L are algebraic over over K.
Note that each element a of K is algebraic over K as it is a root of $x-a=0$.

Example 23. *We know that $\mathbb{C}$ is an extension of $\mathbb{R}$, and $\mathbb{R}$ is an extension of $\mathbb{Q}$.*