Construction of fields of small orders.

1.1. Let F be a field. This means; F is a nonempty set with 2 binary operations defined on it, usually written '$+$' (called addition) and '$\cdot$' (called multiplication) such that the following properties hold:

(i) $(F, +)$ is an abelian group. The (additive) identity is called zero and written '0'.

(ii) $(F \setminus \{0\}, \cdot)$ is also a abelian group. The (multiplicative) identity is called one and written as 1 or 1_F.

(iii) For all $x, y, z \in F$, the following distributive laws hold:

$$x(y+z) = xy + xz; \quad (x+y)z = xz + yz.$$

Ex: $(\mathbb{R}, +, \cdot)$; $(\mathbb{C}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$; for any field F,

$F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], g(x) \neq 0 \right\}$ with usual addition and multiplication; $\mathbb{Z}_p$, p a prime

1.1 Characteristic of a field F.

For any integer $n > 0$, 1_F added to itself n times is written as $n1_F$ or just n if there is no confusion. Thus,

$$1 = 1_F, \quad 2 = 1_F + 1_F, \quad 3 = 1_F + 1_F + 1_F, \ldots$$

If $n \in \mathbb{Z}$, $n < 0$, n (or $n1_F$) denotes -1_F added to itself $-n$ times. Thus,

$$-1 = -1_F, \quad -2 = (-1_F) + (-1_F); \quad -3 = (-1_F) + (-1_F) + (-1_F)$$

etc.

Def. If there exists an integer $n > 0$ such that $n = n1_F$ is zero, ~~we say that F is of~~ the smallest such integer is called the characteristic of F.

If no such integer exists, we say that F is of characteristic zero.

Ex: 1) $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all of characteristic zero.

2) $\mathbb{Z}_p$, p a prime, is of characteristic p.

3) A field F and $F(X)$ have the same characteristic.

Prop: (1) If F is a field of characteristic p, then p is a prime and F contains a subfield F_p isomorphic to $\mathbb{Z}_p$.

(2) If F is a field of characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$. In particular, no finite field can be of characteristic zero.

Proof: (1) If p is not prime and $p = rs$, $1 < r, s < p$, then $r \neq 0 \neq s$, then $0 \neq s = r^{-1}(rs) = r^{-1}p = 0$, a contradiction. So, p is prime. Then, $F_p = \{0, 1, 2, \cdots, p-1\}$ is a subfield of F and isomorphic to $\mathbb{Z}_p$.

(2) If $n1_F \neq 0$ for each positive integer, then $n1_F = -(-n1_F) \neq 0$ for each negative integer n, and so, $\{n1_F : n \in \mathbb{Z}\} \subseteq F$. Since $n1_F \in F \setminus \{0\}$, $(n1_F)^{-1} \in F \setminus \{0\}$ and so $\{(n1_F)^{-1}(m1_F) : m, n \in \mathbb{Z}, n \neq 0\}$ is in F. But this is a subfield of F and is isomorphic to $\mathbb{Q}$. □

Def: A subfield K of a field F is a subset K of F which is a field with respect to the operations in F.

Ex: 1) $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{C}$

2) A field F is a subfield of $F(X)$. □

Cor: If F is a finite field, then $|F| = p^n$ for a prime p and an integer $n > 0$.

Proof. If F is a finite field, then the characteristic of F is a prime p; and F_p is a subfield of F. So, F is a finite dimensional vector space over F_p. So, $\dim_{F_p} F = n$, then $|F| = p^n$. □

Exc. (1) Show that the characteristic of a field is unique.

(2) Give an example of an infinite field of characteristic $\neq 3$.

The converse of the cor. above also true, i.e., for each prime p and an integer $n > 0$, (i) there is a field consisting of p^n elements and (ii) any two fields F_1, F_2 with p^n elements are isomorphic, i.e. $\exists$ a bijection $\theta : F_1 \to F_2$ s.t. $\theta(x+y) = \theta(x) + \theta(y)$ & $\theta(ab) = \theta(a)\theta(b)$ for all $x, y, a, b \in F$ and $a \neq 0 \neq b$.

Because of (i), (ii), We denote a field with p^n elements by $GF(p^n)$ (in honour of E. Galois who first brought out its importance) or F_{p^n}.

A construction of the field F_{p^n} depends on the existence of a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_i \in F_p, \ a_n \neq 0$$

which is irreducible over F_p; i.e., it cannot be written as $f(x) = g(x)\,r(x)$, where $g(x), r(x) \in F_p[x]$, $0 < \deg g(x)$, $\deg r(x) < n$.

The construction

- Let p be a prime number and $\mathbb{F}_p$ denote the field of p elements; Let n be any positive integer and $\mathbb{F}_p^n$ denote the set of all polynomials with coefficients from $\mathbb{F}_p$ and degree less than n; i.e.,

$$\mathbb{F}_p^n = \{f(x) = a_0 + a_1 x + \cdots + a_r x^r : a_i \in \mathbb{F}_p, a_r \neq 0, r < n\}.$$

Thus; $\mathbb{F}_p^n$ is a vector space over $\mathbb{F}_p$ of dimension n. Note that $\{1, x, \ldots, x^{n-1}\}$ is a basis for $\mathbb{F}_p^n$ over $\mathbb{F}_p$.

- Let $p(x) \in \mathbb{F}_p[x]$ be a polynomial of degree n and with coefficients in $\mathbb{F}_p$. We choose $p(x)$ to be irreducible over $\mathbb{F}_p$, i.e., $p(x)$ is not a product of two non constant polynomials of degree less than n.

- **Thm** The set $\mathbb{F}_p^n$ with coordinate addition as the addition of polynomials and multiplication of polynomials taken "modulo $p(x)$" is a field with p^n elements. □

- **Explanation of "modulo $p(x)$".**

If $f(x), g(x) \in \mathbb{F}_p^n$, then $f(x)g(x)$ still has coefficients in $\mathbb{F}_p$ but may be of degree greater than n. But, there exist unique polynomials $r(x), s(x)$ in $\mathbb{F}_p[x]$ such that

$$f(x)g(x) = p(x)r(x) + s(x), \quad \deg s(x) < n.$$

Example. Let $p=2$ and $\mathbb{F}_2=\{0,1\}$. Then,

(i) $\mathbb{F}_2^2[x]=\{0,1,x,1+x\}$. Then, $f(x)=1+x+x^2\in\mathbb{F}_2[x]$ is irreducible over $\mathbb{F}_2$: if it were reducible over $\mathbb{F}_2$, then $(x-0)$ or $(x-1)$ must divide $f(x)$ and so, $x=0$ or $x=1$ is a root of $f(x)$. But $f(0)\neq 0$ and $f(1)\neq 0$. So, $f(x)$ is irreducible over $\mathbb{F}_2$. So, multiplication of elements of $\mathbb{F}_2^2[x]$ modulo $f(x)$ gives a field with 4 elements. The addition in $\mathbb{F}_2^2[x]$ is component wise. The multiplication table is

	1	x	$1+x$
1	1	x	$1+x$
x	x	$1+x$	1
$1+x$	$1+x$	1	x

$x(1+x)=x+x^2=x+x+1$
$=1 \pmod{f(x)}$

$(1+x)(1+x)=1+2x+x^2$
$=1+x^2=x \pmod{f(x)}$

(ii) $\mathbb{F}_2^3[x]=\{0,1,x,x+1,x^2,x^2+1,x^2+x+1,x^2+x\}$
$f(x)=x^3+x+1\in\mathbb{F}_2[x]$ is irreducible over $\mathbb{F}_2$.

	1	x	...	x^2+x+1	x^2+x
1	1	x	. . .	x^2+x+1	.
x	x	x^2	. . .	x^2+1	.
$x+1$	$x+1$	x^2+1	. . .	x	.
x^2	x^2	x^2+1	. . .	1	.
x^2+1	x^2+1	1	. . .	x^2+x	.
x^2+x+1	x^2+x+1	x^2+1	. . .	x^2+x+1	.
x^2+x	x^2+x	x^2+x+1	. . .	x^2	.

$(x^2+x+1)x=x^3+x^2+x$
$=(x+1)+x^2+x$
$=x^2+1 \pmod{f(x)}$

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

$x(x^2+x+1)=x^3+x^2+x$
$=1+x^2 \pmod{f(x)}$

$(x+1)(x^2+x+1)$
$=1+x^2+x^2+x+1 \pmod{f(x)}$
$=x$

$x^2(x^2+x+1) = x[x(x^2+x+1)] = x(1+x) \pmod{f(x)}$

$= x(1+x^2) = x^3+x = 1 \pmod{f(x)}$

FF-6

$(x^2+1)(x^2+x+1) = x^2(x^2+x+1) + (x^2+x+1)$

$= 1 + (x^2+x+1) = x^2+x \pmod{f(x)}$

$(x^2+x+1)(x^2+x+1) = (x^2+1)(x^2+x+1) + x(x^2+x+1)$

$= (x^2+x)+1 = x^2+x+1 \pmod{f(x)}$

$(x^2+x)(x^2+x+1) = x^2(x^2+x+1) + x(x^2+x+1)$

$= 1 + (x^2+1) = x^2 \pmod{f(x)}$

Exc. Complete the multiplication table above.

Example/Remarks:

1) $x^3+x^2+1 \in \mathbb{F}_2[x]$ is (the only one) irreducible polynomial over $\mathbb{F}_2$ of degree 3 (Check these statements). This can also be used to define a multiplication on $\mathbb{F}_2^3[x]$ to get a field with 8 elements. This is different from the above but is isomorphic to the above. (Construct an isomorphism.)

2) Knowing the irreducible polynomials in $\mathbb{F}_2[x]$ over $\mathbb{F}_2$, we can find all irreducible polynomials in $\mathbb{F}_2[x]$ of degree 4 and use any of them to construct a field of 2^4 elements:

~~The Any polynomial~~ $f(x) \in \mathbb{F}_2[x]$ of degree 4 is reducible over $\mathbb{F}_2$ if either it has a factor of degree 1 or of degree 2. So, we get all polynomials $f(x) \in \mathbb{F}_2[x]$ of degree 4 which are irreducible over $\mathbb{F}_2$ ~~all the~~ by removing from the set of all degree 4 polynomials all those which are multiples of irreducible polynomials of degree 1 (i.e., x and $x+1$; equivalently has 0 or 1 as a root) and those of degree 2 (i.e., x^2+x+1)

Polynomials of degree 4 over $\mathbb{F}_2$ (2^4 of them) (FF7)

x^4, x^4+1, x^4+x+1, x^4+x, x^4+x^2+1,
x^4+x^2+x+1, x^4+x^2, x^4+x^3, $x^4+x^3+x^2$,
$x^4+x^3+x^2+1$, x^4+x^3+x, $x^4+x^3+x^2+x$,
x^4+x^3+x+1, $x^4+x^3+x^2+x+1$, $x^4+x^3+x^2+1$
x^4+x^3+1,
of those:

- x^4, x^4+x, x^4+x^2, x^4+x^3, $x^4+x^3+x^2$, x^4+x^3+x
  $x^4+x^3+x^2+x$, x^4+x vanish if you put $x=0$.
- x^4+1, x^4+x^2+x+1, $x^4+x^3+x^2+1$, x^4+x^3+x+1,
  $x^4+x^3+x^2+1$
- $(x^4+x^2+1)=(x^2+x+1)^2$,

So x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$ are the only irreducible over $\mathbb{F}_2$.

Note: You can determine all irreducible polynomials of degree 5 and 6 and so can construct fields of order 2^5 and 2^6. This procedure can be continued.

Exs: (1) Determine irreducible polynomials of degree 2, 3, 4 over $\mathbb{F}_3$.

(2) Same over $\mathbb{F}_5$.

Existence of a polynomial $f(x) \in \mathbb{F}_q[x]$, q a prime power, of degree n and is irreducible over $\mathbb{F}_q$.

For any integer n, denote by $I_q(n)$ denote the number of distinct monic ($\equiv$ leading coefficient 1) polynomials in $\mathbb{F}_q[x]$ of degree n and irreducible over $\mathbb{F}_q$. (Here, $\mathbb{F}_q$ is a field with q elements).

Thm 1. $x^{q^n} - x$ is the product of all distinct monic polynomials in $\mathbb{F}_q$ which are irreducible over $\mathbb{F}_q$ whose degree dividing n. □

Comparing the degrees, we have

Cor 1: $$q^n = \sum_{d|n} d\, I_q(d) \quad \text{---(1)}$$

Möbius inversion formula.

If g and h are functions from $\mathbb{Z}$ to $\mathbb{Z}$ and $h(n) = \sum_{d|n} g(d)$, then

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) h(d) = \sum_{d|n} \mu(d)\, h\left(\frac{n}{d}\right).$$

Proof:

$$\sum_{d|n} \mu(d)\, h\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left[\sum_{b|\frac{n}{d}} g(b) \right] = \sum_{bd|n} \mu(d)\, g(b)$$

$$= \sum_{b|n} g(b) \left(\sum_{d|\frac{n}{b}} \mu(d) \right) = \sum_{b|n} g(b) \left(\sum_{d|\frac{n}{b}} \mu(d) \right) = g(n).$$

because $\sum_{d|\frac{n}{b}} \mu(d) = 0$ unless $\frac{n}{b} = 1$, in which case it is one. □

Taking $h(k) = q^k$ and $g(k) = k I_q(k)$ and applying the Möbius inversion formula, we get

$$n I_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \quad \text{— (2).}$$

• We show that $I_q(n) \neq 0$ for each n. Suppose $I_q(n) = 0$ for some n. Let d' is the smallest integer such that $\mu\left(\frac{n}{d'}\right)$ is non zero. Dividing (2) by $\mu\left(\frac{n}{d'}\right)$, we see that 1 is expressed as a sum of powers of q which is a contradiction. □

Uniqueness of a field of p^n elements

• We describe one of the two methods of proving the uniqueness of a field with p^n elements, p a prime and n a positive integer. In view of this uniqueness, we talk of the finite field of p^n elements and write $\mathbb{F}_{p^n}$ or $GF(p^n)$. Here, "uniqueness" means: if F_1 and F_2 are two fields with $|F_1| = |F_2| = p^n$, then there is a field isomorphism θ from F_1 to F_2; i.e., $\theta : F_1 \to F_2$ is a bijection such that $\theta(x+y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in F_1$.

• The proof of the uniqueness uses the fact that any field K appears as a subfield of an algebraically closed field L such that each element of L is algebraic over K.

Def 1: A field L is said to be algebraically closed if each polynomial $f(x) \in L[x]$ can be written as a product of linear

factors with coefficients in L; in other words, if $f(X) = a_0 + a_1 X + \cdots + a_r X^r$, $a_i \in L$, $a_r \neq 0$, then there exist $\beta, \alpha_1, \cdots, \alpha_r$ such that $f(X) = \beta(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_r)$, $\beta, \alpha_i \in L$.

Def. An element α of L is said to be **algebraic over** K if $f(\alpha) = 0$ for some $f(X) \in K[X]$. (Remember K is a subfield of L. So, $f(\alpha)$ makes sense and $f(\alpha) \in L$).

Ex 1. If $K = \mathbb{Q}$, $L = \mathbb{C}$, any element of K, $\sqrt{2}$, $\sqrt{r}$, $r \in K$ are all algebraic over rationals; but e, π, are not. (difficult theorems)

Th: For a given field K, a field L containing K which is algebraically closed as well as each element of L is algebraic over K exists and unique up to a K-isomorphism of fields. i.e., if L_1 and L_2 are two such fields, there is a field isomorphism $\theta : L_1 \to L_2$ such that $\theta(x) = x$ for each $x \in K$. □

In view of the uniqueness of L given K, we call it the algebraic closure of K and write it as $\overline{K}$.

Ex: 1) $\mathbb{C}$ is algebraically closed. $\mathbb{C}$ has a lot of subfields which is algebraically closed. (Nontrivial to construct such examples!)

2) $\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$

3) $\overline{K}$ is infinite, of same characteristic as K, for **any** field K, including $\mathbb{F}_q$!

- We also recall two other facts you are familiar with in the context of $\mathbb{R}$ or $\mathbb{C}$.

Thm: Let $f(x) \in \bar{K}[x]$ of degree n, Then:

(i) $f(x) = \beta(x-\alpha_1)\cdots(x-\alpha_n)$, $\beta, \alpha_i \in \bar{K}$

(ii) $\alpha \in \bar{K}$ is a root of $f(x)$ and $(x-\alpha)^2$ divides $f(x)$, then α is a root of $f'(x)$ also.

(Recall: If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, by definition, $f'(x) = a_1 + a_2 x + \cdots + n a_n x^{n-1}$.)

Thm: (Existence and uniqueness of a field of order p^n, p any prime and $n \in \mathbb{Z}$, $n > 0$)

Proof. Existence: Consider: $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

Then, $f(x) = (x-\alpha_1)\cdots(x-\alpha_{p^n}) \in \bar{\mathbb{F}}_p[x]$.

because $\bar{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$.

Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_{p^n}\} \subseteq \bar{\mathbb{F}}$. Then:

- $\alpha_i \neq \alpha_j$ for $i \neq j$, because $f'(x) = -1$ and no element of S is a root of $f'(x)$.
- $\mathbb{F}_p \subseteq S$ (by Fermat theorem)
- For $x, y \in S$, $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$ and $(xy)^{p^n} = x^{p^n} y^{p^n}$

So, S is a field containing p^n.

Uniqueness: Elements of any field of order p^n are the roots of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ (?) The algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ and the roots of $f(x)$ in $\bar{\mathbb{F}}_p$ is unique. So, the uniqueness follows. ∎ End.

Thm: Let $q = p^r$, p a prime and $r \in \mathbb{N}$. The multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic.

Proof. We use the following:

(A) For any field K, a polynomial $f(x) \in K[x]$ of degree n has at most n roots in K. In particular, for each $d \mid |\mathbb{F}_q^*|$, $\mathbb{F}_q$ has at most d elements x such that $x^d = 1$.

(B) For each $d \mid n$, $0 \le d \le n$, $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ has a unique subgroup of order d. (In fact, if $s \in \mathbb{Z}$, $1 \le s \le n$, then the subgroup $\langle s \rangle$ is equal to $\langle t \rangle$, where $t = \gcd(n, s)$. To see this, use the fact that there exist integers a and b such that $an + bs = t$.)

(C) For an integer $d \ge 1$, define the Euler number

$$\varphi(d) := \{ s \in \mathbb{Z} : 1 \le s \le d, \ (s, d) = 1 \}.$$

i.e. the images of these integers in $\mathbb{Z}/d\mathbb{Z}$ are the generators of the additive cyclic group $\mathbb{Z}/d\mathbb{Z}$

Lemma. Let $n \in \mathbb{Z}$, $n \ge 1$. Then, $n = \sum_{d \mid n} \varphi(d)$.

Proof of Lemma. For each divisor d of n, let C_d be the unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, and Φ_d be the set of generators of C_d. Since each element of $\mathbb{Z}/n\mathbb{Z}$ generates a cyclic subgroup C_d, $\mathbb{Z}/n\mathbb{Z}$ is the disjoint union of the C_d's. So

$$n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d \mid n} |\Phi_d| = \sum_{d \mid n} \varphi(d). \quad \square$$

(D) Lemma: Let H be a finite group of order n. Suppose that, for each $d \mid n$, there exist at most d elements in H such that $x^d = 1$. Then, H is a cyclic group.

Proof. Let $d \mid n$. If $x \in H$ is of order d, then $\langle x \rangle = \{1, x, \cdots, x^{d-1}, x^d = 1\}$ consists of all elements of H such that $x^d = 1$ and the number of generators of $\langle x \rangle$ is $\varphi(d)$.

So, for each $d \mid n$, the number of elements of H of order d is zero or $\varphi(d)$. This can not be zero for any $d \mid n$ because $|H| = n = \sum_{d \mid n} \varphi(d)$.

In particular, ~~$\varphi(n) \neq 0$ and~~ H contains elements of order n; i.e., H is cyclic. □

Proof of Thm: follows from (A) and (D).

For integrality condition

Prop: Let A and B be real symmetric matrices of order n. Then, there exists a nonsingular matrix D of order n such that $D^t A D$ and $D^t B D$ are diagonal. □

This means that: w.r.t. a suitable basis of $\mathbb{R}^n$, A and B can be written as diagonal matrices; that is: ~~A and B~~ $\mathbb{R}^n$ has a basis $\{f_1, \cdots, f_n\}$ s.t. $Af_i, Bf_i \in \mathbb{R} f_i$, $i = 1, \cdots, n$.

If $Af_i = \lambda_i f_i$, $\lambda_i \neq 0$, we say that f_i is an eigen vector for eigen value λ_i. □