Result (uniqueness):

Let $f(x) \in F[x]$. Any two splitting fields of $f(x)$ over F are isomorphic.

In fact, let $\phi : F \cong F'$ and $f(x) \in F[x]$

If E is a splitting field of $f(x)$ over F

E' is a splitting field of $f(x)$ over F'

then there is isomorphism $\psi : E \longrightarrow E'$ which is an extension of ϕ

$h : A \longrightarrow B$
$C \leq A$
$g : C \longrightarrow B$
$h|_C = g$ (g is restriction of h)

Def:

Let E be an extension of F and $a \in E$.

We call "a" is algebraic over F if a is a zero of some non-zero polynomial over F.

→ If every element of E is algebraic over F then E is algebraic over F.

- If a is NOT algebraic, then it is called TRANSCENDENTAL over F.

→ Let us denote the field of quotients over $F[x]$

$$F[x] = \left\{ f(x)/g(x) \;\middle|\; f(x), g(x) \in F[x],\ g(x) \neq 0 \right\}$$

Remark:

If a is transcendental over F, $F(a) \cong F[x]$

Proof: $\varphi : F[x] \longrightarrow F[a]$, $\varphi(f(x)) = f(a)$

$\overline{\varphi} : F(x)$, $\overline{\varphi}\left(f(x)/g(x)\right) = f(a)/g(a)$

- If a is algebraic then $F(a) \cong F[x]/\langle p(x) \rangle$ where $p(x)$ is a polynomial in $F[x]$ of min. degree s.t $p(a) = 0$, Moreover $p(x)$ is irreducible.

→ Infact, there is unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$

Def: Minimal polynomial of a over F.

- **Result:**

If $[E:F]=n$ then E is algebraic over F.

Proof:

$a \in E$, $[F(a):F] = m$ is finite

$1, a, a^2, \ldots, a^{m-1}$

Is a algebraic extension finite ? ⟶ No

$\mathbb{Q}(A) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots)$ $\quad A = \{\sqrt[n]{2}, n \in \mathbb{N}\}$

Result:

For each prime p and $n \in \mathbb{N}$ then there is a unique field (upto isomorphism) of order p^n.

$GF(p^n)$ called Galois field of order p^n

Result:

As a group under addition, $GF(p^n) = \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ times}}$

As a group under multiplication, $GF(p^n)^* \cong \mathbb{Z}_{p^n-1}$

and hence $GF(p^n)$ is cyclic

→ A field is called prime field if it has no proper subfield.

Remark:

Every field contains a prime field

— Take intersection of all its subfields.

Result:

Prime field of a field F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

Proof:

Take $f: \mathbb{Z} \to F$

$f(n) = n \cdot 1$

If $\ker f = \langle 0 \rangle$ then $\mathbb{Z} \hookrightarrow F$

$\mathbb{Q} \hookrightarrow F$

If $\ker f \neq \langle 0 \rangle$ then $\ker f = \langle m \rangle$

and $\mathbb{Z}/\langle m \rangle \cong \text{Im} f \Rightarrow m$ is prime $\Leftrightarrow$ isID

↳ ID and hence $\mathbb{Z}/\langle m \rangle$ isID

Result:

Number of elements of a finite field is p^n for some prime p and $n \in \mathbb{N}$

Note $\mathbb{Z}_p \hookrightarrow F$

Let $[F : \mathbb{Z}_p] = n$ and $v_1, v_2, \ldots v_n$ be a basis

$\forall\, a \in F$, $a = c_1 v_1 + c_2 v_2 + \ldots + c_n v_n$

so that $|F| = p^n$

Result:

$F = GF(p^n)$

The multiplicative group of non-zero elements of F is cyclic.

F^* is an abelian group of order $p^n - 1$.

Let $\alpha \in F^*$ such that $O(\alpha) = \text{lcm}(O(a))$ $\forall a \in F^*$

↓ denote by r, say

$\Rightarrow a^r = 1 \quad \forall\, a \in F^*$

Recap:

In an abl. group

$O(a) = m$

$O(b) = n$, $\exists c$ $O(c) = \text{lcm}(m,$

As $x^r - 1$ has atmost 'r' zeros in F:

$\Rightarrow |F^*| \leq r$

but $\underbrace{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}}_{\text{all are distinct bcoz order}(\alpha) = r}$ thus we have $|F^*| = r$ and $F^* = \langle \alpha \rangle$

$\therefore F^* = \langle \alpha \rangle$

Corollary: $GF(p^n)^* \cong \mathbb{Z}_{p^n - 1}$

Result:

Any field of order p^n is the splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$

P: The F^* is a multiplicative group of order $p^n - 1$

$\forall\, a \in F^*$, $a^{p^n - 1} = 1$

$\Rightarrow a^{p^n} - a = 0$

Also if $a = 0 \Rightarrow a^{p^n} - a = 0$

Hence every element of F is a zero of $x^{p^n} - x$

As every field is a splitting field $\Rightarrow$ Every field is isomorphic to each other of size p^n.

Result:

If $m|n$, then $GF(p^n)$ has a unique subfield of order p^m. and these are only subfields of $GF(p^n)$

Eg: $GF(16) \longrightarrow GF(2), GF(4), GF(16)$

P: Try as an exercise

Ex: $Z_2[x]/\langle p(x) \rangle = \{ a_0 + a_1 x + a_2 x^2 + \langle \rangle \mid (a_0, a_1, a_2 \in Z_2) \}$

degree 3

$0, 1, a, a^2, \ldots, a^6 \mid 0$

$1 + a + a^2$ Find correspondance between them

Result: [Euler's Theorem]

If $n \geq 1$ and $\gcd(a, n) = 1$

then $\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}$

P:

$U(Z_n) = \{ \bar{a} \mid (a, n) = 1 \}$

$\hookrightarrow$ order $\varphi(n)$

Hence $a^{\varphi(n)} = 1$ in Z_n due to Lagrange's Theorem.

i.e $a^{\varphi(n)} \equiv 1 \pmod{n}$

Corollary: If p is a primes, $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$ [Fermat's Little Theorem]

Result [Wilson's Theorem]:

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$

P: $(\mathbb{Z}_p)^*$ $\quad [x]^2 = [1] \Rightarrow x^2 \equiv 1 \pmod{p}$

i.e $p \mid x^2 - 1$

$p \mid (x+1)(x-1)$

i.e $p \mid (x+1)$ (or) $p \mid x-1$

$\Rightarrow x \equiv 1 \pmod{p}$ (or) $x \equiv -1 \pmod{p}$

$\equiv (p-1) \bmod$

$\overline{1} \times (\underbrace{\overline{2} \times \dots \times}_{\overline{1} \text{ because each element has an inverse in the given set.}}) \overline{p-1}$ $\longrightarrow$ Taken them as numbers

$(p-1)! \equiv (-1) \pmod{p}$

Ex: For $n>1$, if $(n-1)! \equiv (-1) \pmod{n}$ then n is a prime

Def:

AN ARITHMATIC FUNCTION (or) NUMBER-THEORITIC FUNCTION is a function from $\mathbb{N}$ to $\mathbb{R}$ (or) $\mathbb{C}$

Eg:

① Mobinus function (μ)

Defined by $\mu(1) = 1$

and for $n>1$, $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

$$\mu(n) = \begin{cases} (-1)^k & \text{if } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1 \\ 0 & \text{else} \end{cases}$$

Result:

For $n \geq 1$, $\sum_{d \mid n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n=1 \\ 0 & n>1 \end{cases}$

P: If $n=1$, it is clear

If $n>1$ let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\sum_{d \mid n} \mu(d) = 1 + \mu(p_1) + \mu(p_2) + \dots + \mu(p_k) + \mu(p_1 p_2) + \dots + \mu(p_{k-1} p_k) + \mu(p_1 p_2 \dots p_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2} 1 + \dots = 0$$

Def:

For f, g two arithmatic functions define

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

Denote $h = f * g$, called Dirichlet Product

Remark:

1) $*$ is commutative
2) $*$ is associative (try this as an exercise)

→ $f * I = f$

i.e $\sum_{d|n} f(d) I\left(\frac{n}{d}\right) = f(n) \quad \forall n$

$f(n) I(1) + \ldots$

$\Rightarrow \boxed{I(n) = \left[\frac{1}{n}\right]}$

→ $f * f^{-1} = I$

i.e $\sum_{d|n} f(d)\, f^{-1}\left(\frac{n}{d}\right) = \left[\frac{1}{n}\right] \quad \forall n$

For $n=1$, $f(1) * f^{-1}(1) = 1 \Rightarrow f^{-1}(1) = \frac{1}{f(1)}$

*So, for inverse to exist, $f(1) \neq 0$

For $n>1$, $\sum_{d|n} f(d)\, f^{-1}\left(\frac{n}{d}\right) = 0$

$$\Rightarrow f(1) \cdot f^{-1}(n) + \sum_{\substack{d|n \\ d>1}} f(d)\, f^{-1}\left(\frac{n}{d}\right) = 0$$

$$\Rightarrow f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d) f^{-1}\left(\frac{n}{d}\right)$$

- Arithmatic functions under dirchilet's product forms a monoid.
  If $f(1) \neq 0$, it forms an Abelian group.

Midsem solutions:

(1) $n = (a_k a_{k-1} \cdots a_1 a_0)_{10}$

$P(x) = \sum_{i=1}^{k} a_i x^i$ $\quad P(10) = n$

Note $10 \equiv -1 \pmod{11} \Rightarrow P(10) = n = \sum_{i=1}^{k} (-1)^i \pmod{11}$

---

(2) $a, a+b, a+2b, \ldots$ AP

~~a+np~~ $a + nb = p$

$a + $ ~~nk~~ $(n+kp) = a+nb+kpb$ is composite $\forall k$

---

(3) $K \leq H \leq G$

$[G:H] = \frac{|G|}{|H|}$ by lagrange's theorem.

$[G:H][H:K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G:K]$

---

(4) $(a,b) \in G \times H$

Let $O(a,b) = k$

$(e,e) = (a,b)^k = (a^k, b^k)$

$\Rightarrow a^k = e \;\&\; b^k = e \Rightarrow O(a) \mid k$ and $O(b) \mid k$

As k is least, $O(a,b) = \text{lcm}(O(a), O(b))$

---

(5) $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\Leftrightarrow \gcd(m,n) = 1$

$\Rightarrow$ Let $\langle (g,h) \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$ $\quad \gcd(m,n) = d$.

$(g,h)^{mn/d} = \left((g^m)^{n/d}, (h^n)^{m/d} \right) = (e,e)$

$mn \mid \frac{mn}{d} \Rightarrow d = 1$

$\Leftarrow$ Let $\mathbb{Z}_m = \langle a \rangle$, $\mathbb{Z}_n = \langle b \rangle$

Now $O(a,b) = \text{lcm}(O(a), O(b)) = \text{lcm}(m,n) = mn$

$\Rightarrow \langle (a,b) \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$

---

(6) $H \leq G$

$x \in G$ $\quad xHx^{-1} = H$

↳ it is a subgroup & cardinality of $xHx^{-1} = |H|$

$\Rightarrow$ Only one of this size $\Rightarrow$ H is NORMAL

---

(7) $|G| = p^n$

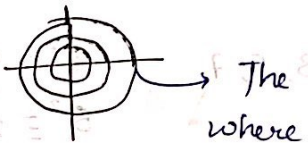
Take any non-trivial element $a \in G$ then $\langle a \rangle \leq G$ (size p^k)

$|H| = p$

---

(8) $\mathbb{C}^*/N \cong \mathbb{R}^+$

$N \hookrightarrow \{x \mid |x| = 1\}$



The +ve real number where the circle cuts +ve X-Axis is the representative

$f : \mathbb{C}^* \longrightarrow \mathbb{R}^*$

$f(z) = |z|$

---

(9) Atleast $n+1$ primes $< 2^{2^n}$

$p_{k+1} \leq p_1 p_2 \cdots p_k + 1$

---

(10) $p = p_1 + p_2$, $p = p_3 - p_4$

i.e $p = p_1 - 2$, $p = p_3 - 2$

---

(11) $23x \equiv 51 \pmod{60}$

Here $x = 57$

---

(12) $n \equiv 1 \pmod 2$, $n \equiv 2 \pmod 4$, $n \equiv 3 \pmod 5$

$n \equiv 238 \pmod{60}$ $\therefore$ Answer is 58

Result: For $n \geq 1$, $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

$p \mid n$ → prime divisor

Proof: Let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of n

$$\prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= 1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i,j} \frac{1}{p_i p_j} - \sum_{i,j,l} \frac{1}{p_i p_j p_l} \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}$$

For each term, its μ value is in the numerator

$$= \sum_{d \mid n} \frac{\mu(d)}{d}$$

→ 1) For any $\alpha \geq 1$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

2) $\varphi(mn) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}$ where $d = gcd(m,n)$

3) $a \mid b \Rightarrow \varphi(a) \mid \varphi(b)$

4) $\varphi(n)$ is even for all $n \geq 3$

$(a,n) = 1$

$n = 8$: $a = 1, 3, 5, 7$ $\quad 3^2 \equiv 9 \equiv 1 \pmod 8$

$5^2 \equiv 25 \equiv 1 \pmod 8$

$7^2 \equiv 49 \equiv 1 \pmod 8$

→ $U(\mathbb{Z}_n) = \{a \mid (a,n) = 1\}$

↓ units

$|U(\mathbb{Z}_n)| = \varphi(n)$

Checking U_n is cyclic or NOT i.e $U_n = \langle a \rangle$ ↳ generator

if cyclic $U_n = \{1, a, \ldots, a^{\varphi(n)-1}\}$

Def:

Let $(a,n) = 1$, the least k such that

$a^k \equiv 1 \pmod n$

is called the Exponent of $a \bmod n$, represented by $O(a)$ or $exp_n(a)$.

- $n = 9$: $a = 1, 2, 4, 5, 7, 8$

For 2, $1, 2, 4, 8, 16, 32, 64$

$\equiv 1, 2, 4, 8, 7, 5, 1 \pmod 9$

For 5, $1, 5, 25, 125, 625, 3125$

$\equiv 1, 5, 7, 8, 4, 2 \pmod 9$

For 7, $1, 7, 49, 343$

$\equiv 1, 7, 4, 1 \pmod 9$

* <a> = If U_n is cyclic, then the no. of generators of U_n is $\varphi(\varphi(n))$

and they are $\{ a^k \mid 1 \le k \le \varphi(n), (k, \varphi(n)) = 1 \}$

Def:

If U_n is generated by a, then we call a PRIMITIVE ROOT of n if $exp_n(a) = \varphi(n)$

- For what n, we have primitive roots?

$1, 2, 4, p^\alpha, 2p^\alpha$ $\forall$ $\alpha \ge 1$ and p: odd prime

2^α, $\alpha \ge 3$ has no primitive root

Result: Let x be odd, if $\alpha \ge 3$

$$x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$$

Proof: By induction on α

Basis $\longrightarrow$ For $\alpha = 3$, see left

I.H $\longrightarrow$ Assume the result for α i.e $x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$

I.S $\longrightarrow$ From I.H,

$$x^{\varphi(2^\alpha)/2} = t \cdot 2^\alpha + 1$$

Squaring on both sides

$$\Rightarrow x^{\varphi(2^\alpha)} = t^2 \cdot 2^{2\alpha} + 2^{\alpha+1} \cdot t + 1$$

$$\Rightarrow x^{\varphi(2^\alpha)} \equiv 1 \pmod{2^{\alpha+1}}$$

$$\Rightarrow x^{\varphi(2^{\alpha+1})/2}$$

Result: If $(m, n) = 1$; $m > 2$ and $n > 2$ then mn has no primitive root

Proof: Let $(a, mn) = 1 \Rightarrow (a, m) = 1$ & $(a, n) = 1$

From Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$

$$\Rightarrow \left(a^{\varphi(m)}\right)^{\varphi(n)/d} \equiv 1 \pmod{m} \quad \text{where } d = \gcd(\varphi(m), \varphi(n))$$

$$\Rightarrow a^k \equiv 1 \pmod{m} \quad k = \operatorname{lcm}(\varphi(m), \varphi(n))$$

Similarly, $a^k \equiv 1 \pmod{n}$

As $(m,n)=1$, $a^k \equiv 1 \pmod{mn}$

$$k = \frac{\varphi(m)\cdot\varphi(n)}{d} = \frac{\varphi(mn)}{d}$$

As $\varphi(m), \varphi(n)$ both are even $\Rightarrow d \geq 2$

$$\Rightarrow k = \frac{\varphi(mn)}{d} \leq \frac{\varphi(mn)}{2}$$

Claim: If p is odd prime and $\alpha \geq 1$
Suppose p^α has primitive root, we claim that $2p^\alpha$ has a p.root

Proof: Let a be a primitive root of p^α

If a is even, note that $a+p^\alpha$ is also a primitive root of p^α
↳ odd number

Let b be a odd primitive root of p^α (Note $(b, 2p^\alpha)=1$)
and let $k = \exp_{2p^\alpha}(b) \Rightarrow k \mid \varphi(2p^\alpha)$

$b^k \equiv 1 \pmod{2p^\alpha} \Rightarrow b^k \equiv 1 \pmod{p^\alpha}$

$\Downarrow$

$\varphi(p^\alpha) \mid k$

As $\varphi(2p^\alpha) = \varphi(2)\cdot\varphi(p^\alpha)$
$= \varphi(p^\alpha)$ $\Rightarrow \varphi(p^\alpha) \mid k \Rightarrow \varphi(2p^\alpha) \mid k$

$\therefore k = \varphi(2p^\alpha)$

* Let a be a primitive root of n

$a, a^2, \ldots, a^{\varphi(n)}$ $\quad (b,n)=1$

For $(b,n)=1$, there is a unique k such that

$$b \equiv a^k \pmod{n}$$

We call k is the INDEX OF b to the BASE a

$$\text{ind}_a b = k$$

Properties:

① $\text{ind}_a(xy) = \text{ind}_a(x) + \text{ind}_a(y) \pmod{\varphi(n)}$.

② $k>0$, $\text{ind}_a(x^k) = k\,\text{ind}_a(x) \mod(\varphi(n))$

③ $\text{ind}_a(a) \equiv 1 \mod(\varphi(n))$

$\text{ind}_a(1) \equiv 0 \mod(\varphi(n))$

→ Let p be an odd prime

$\forall\, \alpha \geq 1$ p^α has a primitive root

Proof: p has a primitive root

because $\mathbb{Z}_p^*$ is cyclic.

Let 'a' be a primitive root mod p

$a^{p-1} \equiv 1 \pmod p$ $\quad[\because \varphi(p) = p-1]$

If $a^{p-1} \equiv 1 \pmod{p^2} \Rightarrow$ then 'a' is NOT primitive root of p^2.

Hence, for any primitive root 'a' of p to be a primitive root of p^2

then $a^{p-1} \not\equiv 1 \pmod{p^2}$

Result: Let a be a primitive root mod p

a is p.r of p^α $\forall\, \alpha \geq 1 \iff a^{p-1} \not\equiv 1 \pmod{p^2}$

Proof: $\Rightarrow$: Take $\alpha = 2$, then clearly $a^{p-1} \not\equiv 1 \pmod{p^2}$

$\Leftarrow$: First observe that p has a p.r 'a' satisfying

$$a^{p-1} \not\equiv 1 \pmod{p^2} \longrightarrow (\star)$$

Let 'b' be a arbitrary p.r of p

If b satisfies $\star$, then we are done

If not, $b^{p-1} \equiv 1 \pmod{p^2}$

in this case, consider $b_1 = b + p$ is the p.r of p.

$$b_1^{p-1} = (b+p)^{p-1}$$

$$= b^{p-1} + (p-1)b^{p-2}\cdot p + tp^2$$

$$= b^{p-1} - pb^{p-2} + t'p^2$$

$$\equiv b^{p-1} - pb^{p-2} \pmod{p^2}$$

$$\equiv 1 - pb^{p-2} \pmod{p^2} \quad \left[\text{As } b^{p-2} \not\equiv 0 \pmod p,\ pb^{p-2} \not\equiv 0 \pmod{p^2}\right]$$

$$\Rightarrow b_1^{p-1} \not\equiv 1 \pmod{p^2}$$

Let 'a' be a primitive root of p such that

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

Let $k = O(a) \bmod p^\alpha$

Claim: $k = \varphi(p^\alpha)$

$a^k \equiv 1 \bmod p^\alpha$, we have $a^k \equiv 1 \pmod{p}$

$\Rightarrow \varphi(p) \mid k$

$\Rightarrow k = q\varphi(p)$.

As $k \mid \varphi(p^\alpha) \Rightarrow q\varphi(p) \mid \varphi(p^\alpha)$

$\Rightarrow q(p-1) \mid p^{\alpha-1}(p-1)$

$\Rightarrow q \mid p^{\alpha-1}$

Let $q = p^\beta$, when $\beta \leq \alpha - 1$

Claim: $\beta = \alpha - 1$ so that $k = \varphi(p^\alpha)$

Suppose $\beta \leq \alpha - 2$.

$$\left[k = p^\beta(p-1)\right] \mid \left[p^{\alpha-2}(p-1) = \varphi(p^{\alpha-1})\right]$$

Hence $\varphi(p^{\alpha-1})$ is a multiple of k

$\Rightarrow a^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$

For $\alpha = 2$, this is NOT possible as $a^{p-1} \not\equiv 1 \pmod{p^2}$

↳ For $\alpha > 2$, prove it by induction. (exercise)