Algebra I Fields (13.1):

Pf: By Fund. theorem, the finite subgp. is $\cong$ to

$\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$, $n_k \mid n_{k-1} \mid \dots \mid n_2 \mid n_1$

Thus, n_k divides orders of each (cyclic) factor x_i; when $\Rightarrow$ (gen. fact. about cyclic gps) each factor has n_k elts of order dividing n_k.

If $k > 1$, there would be more than n_k elts

$\Rightarrow$ more than n_k roots of $x^{n_k} - 1$ in F $\#$.

Thus, $k = 1 \Rightarrow$ cyclic gp.

Cor: p prime $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

A few small collection of these ideas in the book.

Fields (not our focus)

Characteristic of F $ch(F)$: smallest $n \in \mathbb{N}$ s.t. $n \cdot 1 = 0$ or $n = 0$.

$ch(F) = 0$ if $\nexists\, n \in \mathbb{N}$, $n \cdot 1 = 0$.

If $ch(F) \neq 0$ (called finite characteristic), then $ch(F)$ is prime, as if $ch(F) = n = a \cdot b$, $1 < a, b < n$, then

$n \cdot 1 = (a \cdot b) \cdot 1 = (a \cdot 1)(b \cdot 1) = 0 \Rightarrow a \cdot 1 = 0$ or $b \cdot 1 = 0$

~~Contradicts minimality~~ minimality

If $ch(F) = p$, then $p \cdot \alpha = 0 \; \forall \alpha \in F$, as

$p \cdot \alpha = p \cdot (1 \cdot \alpha) = (p \cdot 1) \cdot \alpha = 0 \cdot \alpha = 0$.

(1)

(N.B: $ch(R)$ makes sense for domains R, $ch(R) = ch(\text{field of fracs})$.)

Ex: $ch(\mathbb{Q}) = ch(\mathbb{R}) = ch(\mathbb{C}) = 0$.

- $\mathbb{Z}/p\mathbb{Z}$ has char. p.
- Finite fields $\mathbb{F}_{p^n}$ of char. p. (construct later).
- $\mathbb{Z}/p\mathbb{Z}(x)$ rat'l fcns
  $((x))$ Laurent series
  are char. p.

Recall: Ideals in fields are trivial

$\Rightarrow$ ring homs. b/w fields are trivial or injective.

New pts

$\varphi: \mathbb{Z} \to F$

$n \longmapsto n \cdot 1$

$\ker(\varphi) = ch(F) \cdot \mathbb{Z}$

$\rightsquigarrow$ $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ injects into F.

Thus $\Rightarrow$ F contains a copy of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, (fld of fracs) (already field)

the prime subfield, gen. by 1.

Thus, the study of field maps is the study of field ext^{ns}.

K
$|$
F $\quad K/F$ K over F means $F \subseteq K$ is a subfield.

~~In this situat~~ Here, note that K is an F-vector space.

Pf: $[K:F]$ is the dim^{n} of this vector space
↑ degree of ext^{n}

Ext^{n} by adjoin roots of polys:

Th If $p(x) \in F[x]$ irred.
Then there is a field K (ext) where $p(x)$ has a root.

F ~~("Isomorphic copy")~~

Pf: Take $K = F[x]/(p(x))$ ← ideal gen. by $p(x)$.
$F[x]$ is a PID.
$p(x)$ irreducible $\Leftrightarrow$ prime $\overset{\text{PID}}{\Rightarrow}$ maximal $\Rightarrow K$ is a field.
projection: $\pi : F[x] \twoheadrightarrow K$
$f \longmapsto \bar{f} \pmod{(p(x))}$.
$\pi|_F : F \to K$ is not trivial as
$1 \mapsto 1$
$\Rightarrow$ its injective $\Rightarrow$ a copy of F is in K.
We Identify ~~F~~ $F \cong \pi|_F(F)$, ~~we find~~: Now, $\bar{x} = \pi(x)$

$$\begin{aligned} p(\bar{x}) &= \overline{p(x)} \qquad (\pi \text{ is a hom.}) \\ &= p(x) \pmod{p(x)} \\ &= 0 \end{aligned}$$

$\Rightarrow \bar{x} = \pi(x)$ is a root of $p(x)$.

Ex: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ $x^2+1=0$ in quotient, or $x^2 = -1$.
already algebraically closed! Very surprising!
cut [Fund. Th $=$ of Alg: neither fund. nor usually proven in alg.

Th: $p \in F[x]$ irred. of deg. n, $K = F[x]/(p(x))$, $\vartheta = \bar{x} \in K$.
Then $[K:F] = n$, with basis $1, \vartheta, \ldots, \vartheta^{n-1}$.

If: Take any $a(x) \in F[x]$. $F[x]$ is Euclidean, so $\exists q, r$

$$a(x) = p(x)\cdot q(x) + r(x) \qquad \deg(r) < n.$$

$q \cdot p \in (p) \Rightarrow a \equiv r \bmod (p)$.

$\Rightarrow$ every res. class in K is rep. by a poly of deg $< n$.

$\Rightarrow 1, \vartheta, \ldots, \vartheta^{n-1}$, the images of $1, x, x^2, \ldots, x^{n-1}$ span K/F.

If they weren't linearly ind./K, say

$$b_0 + \ldots + b_{n-1}\vartheta^{n-1} = 0, \text{ not all } b_i = 0.$$

$$\Leftrightarrow b_0 + \ldots + b_{n-1}x^{n-1} \equiv 0 \bmod (p(x))$$

$$\Leftrightarrow p(x) \mid (b_0 + \ldots + b_{n-1}x^{n-1}) \quad *.$$

($p(x)$: deg. n; $b_0 + \ldots + b_{n-1}x^{n-1}$: deg $< n$) $\Rightarrow$ basis.

Cor: In K, if $a(\vartheta), b(\vartheta) \in K$, addition is poly. addition, and

$a \cdot b = r$, where r is remainder of $a \cdot b$ divided by p in $F[x]$.

Ex: $p(x) = x^2+1$, but $F = \mathbb{Q}$.

$\rightsquigarrow \mathbb{Q}(i)$ adjoins a root.

~~"Non-Galois example"~~

Ex: $F = \mathbb{Q}$, $p = x^3 - 2$ irred. by Eisenstein at 2. ~~MISSED other roots!~~

Take a root ϑ: $\Rightarrow \mathbb{Q}(x)/(x^3-2) \cong \{a_1 + a_2\vartheta + a_3\vartheta^2 / a_i \in \mathbb{Q}\}$

where $\vartheta^3 = 2$. deg. 3 ext.

Sample inverse: $1+\vartheta$: $a(x)\cdot(1+x) + b(x)(x^3-2) = 1$ inverse is $a(x) = \frac{1}{3}(x^2-x+1)$

Euc. Alg.: $\mathbb{Z}$ ... (lower degree)

$\Rightarrow (1+\vartheta)^{-1} = \frac{\vartheta^2 - \vartheta + 1}{3}$

Def: $\begin{matrix} K \\ | \\ F \end{matrix}$ $\alpha, \beta, \ldots \in K$ $F(\alpha, \beta, \ldots)$

field gen. by $\alpha, \beta, \ldots / F$

smallest subfield:

$$\begin{matrix} K \\ | \\ \alpha, \beta, \ldots \in F(\alpha, \beta, \ldots) \\ | \\ F \end{matrix}$$

further

If $K = F(\alpha)$, then

K is a simple ext, α is a primitive el't.

Th: $p \in F[x]$ irred., K/F contains a root α of $p(x)$.

Then $F(\alpha) \cong F[x]/(p)$. (α gen. by α.)

Pf: Natural hom: $\varphi: F[x] \to F(\alpha) \subseteq K$

$a(x) \longmapsto a(\alpha)$.

i.e. send $x \mapsto \alpha$ and extend linearly

just say out loud

00 proof

$p(\alpha) = 0$ by assumpt. $\Rightarrow p(x) \in \ker(\varphi)$ (same kernel)

$\Rightarrow$ induced hom. $\varphi: F[x]/(p) \to F(\alpha)$.

(p) irred. $\Rightarrow$ domain is a field, not trivial hom.

$\Rightarrow F[x]/(p) \cong \varphi(F[x]/(p)) \subseteq F(\alpha)$.

subfield of $F(\alpha)$ containing F, α $\Rightarrow$ φ is surjective

(5) smallest such $\Rightarrow$ ☐

Assume the notation above.

Cor: If p has deg. n,

$$F(\alpha) = \{a_0 + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in F\} \subseteq K.$$

Next time: ~~further examples~~

Extra time! (finish §13.1).

Classical constructions: —

double the cube...

Comments on exam