

# Fields Review + Exam problems.

$F$  a field has two operations  $+$ ,  $\cdot$   
 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ , finite fields  $GF(q)$   $q$  prime power.

both commutative  
both have inverses  
(Section 19)

Constructions of fields:

- 1)  $R$  integral domain  $\Rightarrow F_R$  field of fractions (Section 21)  
(commutative ring with unity  $1_R$ )  
no zero divisors
- 2)  $R$  commutative ring with unity and  $I$  maximal ideal  
then the quotient ring  $R/I$  is a field (Section 27)

Recall. An ideal  $I \subseteq R$  is a additive subgroup of  $(R, +)$  such that  $\forall a \in R \quad aI, Ia \subseteq I$

If  $R$  is commutative enough to ask  $aI \subseteq I \quad \forall a \in R$ .

$I$  is a maximal ideal of  $R$  if  $\nexists J$  ideal of  $R$   $\frac{s.t.}{I \subsetneq J \subsetneq R}$

2\*  $F$  a field then  $F[x] = R$  then

$\langle f(x) \rangle = \{ g(x) \cdot f(x) \mid g(x) \in F[x] \}$  "principal ideal generated by  $f(x)$ "

is maximal ideal  $\iff f(x)$  is irreducible over  $F$

$\frac{F[x]}{\langle f(x) \rangle}$  is a field  $\iff f(x)$  is irreducible over  $F$

The field  $E = F[x] / \langle f(x) \rangle$  contains a zero  
 $\alpha$  of  $f(x)$  and a subfield isomorphic to  $F$ .  
 $\cong x + \langle f(x) \rangle$

distinct coset representatives.

$$E = \frac{F[x]}{\langle f(x) \rangle} = \{ g(x) + \langle f(x) \rangle \mid g(x) \in F[x] \}$$

with operations

well defined since  
 $(R, +)$  is abelian  
 have  $I \triangleleft (R, +)$   
 is normal

$$(g(x) + \langle f(x) \rangle) + (h(x) + \langle f(x) \rangle) := g(x) + h(x) + \langle f(x) \rangle$$

$$(g(x) + \langle f(x) \rangle) \cdot (h(x) + \langle f(x) \rangle) := g(x)h(x) + \langle f(x) \rangle$$

well defined since  
 $I$  is an ideal ( $aI \subseteq I$ )

Exam 2020 Problem 4 (NOTE THIS WAS A ONE WEEK EXAM!)

$F = \mathbb{Z}_3$  and  $f(x) = x^3 + 2x + 1 \in F[x]$

4a Explain why  $K = F[x] / \langle f(x) \rangle$  is a field.

$K$  is a field iff  $\langle f(x) \rangle$  is a maximal ideal in  $F[x]$   
iff  $f(x)$  is irreducible over  $F$ .

Since  $f(x)$  is of degree 3 if it is reducible over  $F$   
it must have a zero in  $F = \{0, 1, 2\}$ .

However,  $f(0) = 1$   $f(1) = 1 + 2 + 1 = 1$   $f(2) = 8 + 4 + 1 = 1$

so there is no zero of  $f(x)$  in  $F$  Hence  $f(x)$  is  
irreducible over  $F$  and  $K$  is a field.

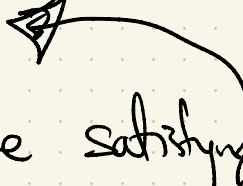
**NOT PART OF EXAM** elts of  $K$  are  $\{g(x) + \langle f(x) \rangle\}$ ?

$$x^3 + \langle x^3 + 2x + 1 \rangle \stackrel{(*)}{=} x^3 + (-x^3 - 2x - 1) + \langle x^3 + 2x + 1 \rangle$$

Since recall

$$= -2x - 1 + \langle x^3 + 2x + 1 \rangle.$$

$$g(x) + \langle f(x) \rangle = g'(x) + \langle f(x) \rangle \iff g(x) - g'(x) \in \langle f(x) \rangle$$

Notice by adapting  $(*)$  we can always find a coset representative  $g(x)$  with  $\deg(g(x)) < \deg(f(x))$  

Moreover we showed that the representative satisfying  $(*)$  is unique.

Compare this to  $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z}\}$  ← to uniquely represent a coset restrict to  $0 \leq a \leq n-1$

$$E = \frac{F[x]}{\langle f(x) \rangle} \cong F(\alpha) = \left\{ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid \begin{array}{l} a_i \in F \\ \deg f = n \end{array} \right\}$$

with  $\rightarrow$  set of cosets  
+ and -

↑  
"Simple extension"  
of  $F$

and where

$$\alpha^n = -\sum_{i=0}^{n-1} b_i \alpha^i \quad \text{where}$$

isomorphism is given by:  $f(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$ .

$$g(x) + \langle f(x) \rangle \mapsto g(\alpha).$$

$$\deg g(x) < n = \deg f$$

Notice  $E$  contains a subfield isomorphic to  $F$  namely

$\{a_0 + \langle f(x) \rangle\}$  notice this is sent to  $F \subseteq F(\alpha)$   
 $\uparrow$   
 all  $a_i = 0 \quad i > 0$ .

A field extension  $E$  of  $F$  just means a field  $E$  containing  $F$ .

BONUS: If  $E$  is an extension of  $F$  then  $E$  is a vector space over  $F$ .

$\dim$  of  $E$  over  $F$  is called the degree of  $E$  over  $F$  and denoted it by  $[E:F]$ .

Eg  $E = F(\alpha)$  with  $\alpha$  algebraic over  $F$ .  
( $\exists f(x) \in F[x]$  with  $\alpha$  a zero)

Then  $\dim$  of  $E$  over  $F$  as a vector space is  $\deg \text{irr}(\alpha, F)$

⚠  $f(x)$  does not necessarily split over  $F(\alpha)$ .

Example  $f(x) = x^4 - 2$

Zeros in  $\mathbb{C}$ :  $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$

$f(x)$  is irreducible /  $\mathbb{Q}$   
by Eisenstein  $p=2$

$E = \frac{\mathbb{Q}[x]}{\langle f(x) \rangle} \cong \mathbb{Q}(\alpha)$  for any zero  $\alpha$ .

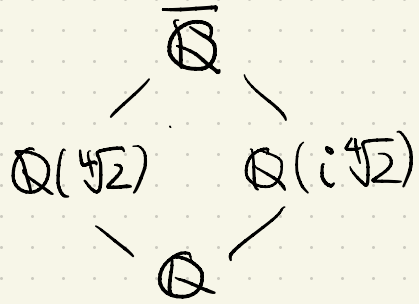
$\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(-\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2}) = \mathbb{Q}(-i\sqrt[4]{2})$ .

$\cap$   
 $\mathbb{R}$

$\nmid$   
 $\mathbb{R}$ .

equalities  
are as  
subfields  
of  $\overline{\mathbb{Q}}$  (or  $\mathbb{C}$ )

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$



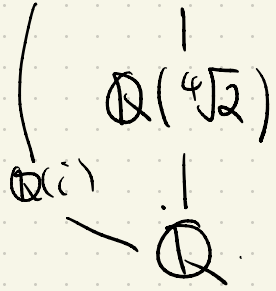


The splitting field  $K$  of  $f(x)$  must contain all 4 zeros.

$$\mathbb{Q}(\sqrt[4]{2})$$

$$\mathbb{Q}(\sqrt[4]{2}, i) = K = \mathbb{Q}(\sqrt[4]{2})(i)$$

$$\text{irr}(i, \mathbb{Q}(\sqrt[4]{2})) = x^2 + 1$$



$$\begin{aligned} [K:\mathbb{Q}] &= [K:\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] \\ &= 2 \cdot 4 = 8 \end{aligned}$$

$$G(K/\mathbb{Q}) = \{\rho_0, \dots, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$$

$\{K:\mathbb{Q}\} \leftarrow$  index of the field ext'n.  
 " # of ext'ns of  $\sigma:\mathbb{Q}\rightarrow\mathbb{Q}$  to  $\mathbb{C}$   
 $\tau:K\rightarrow\tau(K)$

54.5 Table  $\equiv id$

*complex conjugation*

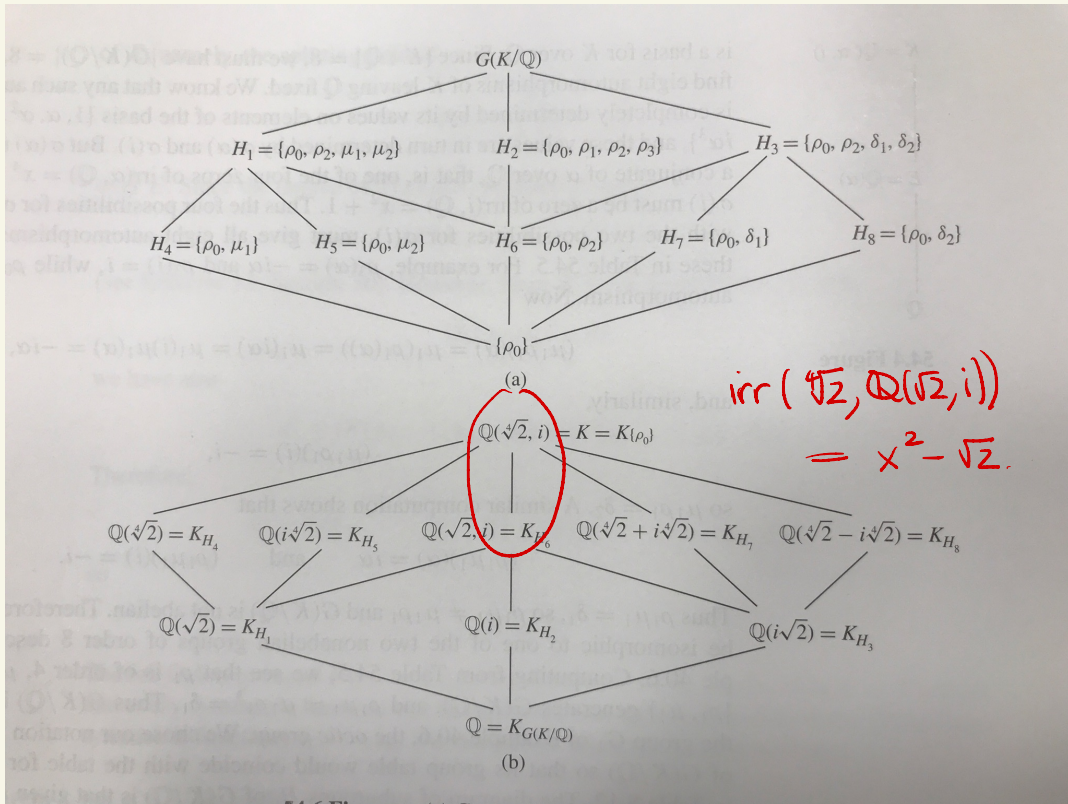
	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\delta_1$	$\mu_2$	$\delta_2$
$\alpha \rightarrow$	$\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$	$\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$
$i \rightarrow$	$i$	$i$	$i$	$i$	$-i$	$-i$	$-i$	$-i$

$$\alpha = \sqrt[4]{2}$$

When  $K$  is a splitting field then

$$\{K:\mathbb{Q}\} = |G(K/\mathbb{Q})|$$

" *separable*  
 $[K:\mathbb{Q}]$  *ext'n.*



Exam 2016 Problem 2  $K$  is the splitting field of

$$f(x) = (x^3 - 8)(x^2 - 2) \in \mathbb{Q}[x].$$

1) Find the degree  $[K:\mathbb{Q}]$  and the group  $G(K/\mathbb{Q})$

$$f(x) = (x-2)(x^2+2x+4)(x^2-2) \quad / \quad \mathbb{Q}.$$

$x^2-2$  has roots  $\sqrt{2}, -\sqrt{2}$

$x^2+2x+4$  has zeros  $r = \frac{-2 \pm \sqrt{4-16}}{2} = \frac{-2 \pm 2i\sqrt{3}}{2} = -1 \pm i\sqrt{3}$

The zeros of  $f(x)$  are  $2, \sqrt{2}, -\sqrt{2}, -1 \pm i\sqrt{3}$ .

Therefore  $K = \mathbb{Q}(\sqrt{2}, -1+i\sqrt{3}) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$

$i\sqrt{3} \in \mathbb{Q}(\sqrt{2})(-1+i\sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{2}, i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, -1+i\sqrt{3})$

$-1+i\sqrt{3} \in \mathbb{Q}(\sqrt{2}, i\sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{2}, -1+i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, i\sqrt{3})$

$K = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$

$[\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2 = \deg(x^2 + 3)$   
"ir"( $i\sqrt{3}, \mathbb{Q}(\sqrt{2})$ )

$\mathbb{Q}(\sqrt{2})$

$\mid$

$\mathbb{Q}$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$   
 $= \deg(x^2 - 2)$

so  $G(K/\mathbb{Q})$  is

$[K : \mathbb{Q}] = 4$  Hence  $|G(K/\mathbb{Q})| = 4$ .  $\mathbb{Z}_4$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2$

$G \in G(K/\mathbb{Q})$  must send  $\alpha$  to a conjugate. Hence

$$\sqrt{2} \mapsto \pm\sqrt{2} \quad \text{so} \quad G^2 = \text{id} \quad \forall G \in G(K/\mathbb{Q})$$

$$i\sqrt{3} \mapsto \pm i\sqrt{3}$$

there is no element of

order 4 so  $G(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

2b) Find an elt  $a \in K$  st  $K = \mathbb{Q}(a)$ .

$$\text{let } \beta = \sqrt{2} \quad \beta' = -\sqrt{2} \quad \alpha = i\sqrt{3} \quad \alpha' = -i\sqrt{3}$$

By the primitive elt theorem proof find

$$c \in \mathbb{Q} \text{ st. } c \neq \frac{2\sqrt{2}}{2i\sqrt{3}}$$

$$a = \sqrt{2} + c i\sqrt{3} \quad \text{ie take } c = 1.$$

claim  $\mathbb{Q}(\sqrt{2} + i\sqrt{3}) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ .

$$\mathbb{Q}(\sqrt{2} + i\sqrt{3})$$

$$\mathbb{Q}.$$

Claim  $[\mathbb{Q}(\sqrt{2} + i\sqrt{3}) : \mathbb{Q}] = 4$ . It can only be

1, 2, 4. However, if 2 then  $1, a$

$a^2 = -1 + i\sqrt{6}$ .  $\nrightarrow$  cannot be written as

$r + sa$  for  $a, r \in \mathbb{Q}$ .

Hence  $\mathbb{Q}(\sqrt{2} + i\sqrt{3}) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ .





