HW 3 due this Fri

HW 4 due Fri Mar 23.

Exam 2 Wed Mar 28.

Today: Splitting Fields.

Given field extension $F \subseteq K$ with $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ we define

$$F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$$

$$F(\alpha_1, \alpha_2, \alpha_3) = (F(\alpha_1, \alpha_2))(\alpha_3)$$

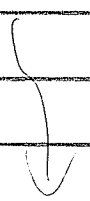
$$\vdots$$

$$F(\alpha_1, \ldots, \alpha_n) = (F(\alpha_1, \ldots, \alpha_{n-1}))(\alpha_n).$$

= the smallest subfield of K containing $F \cup \{\alpha_1, \ldots, \alpha_n\}$.

Alternatively,

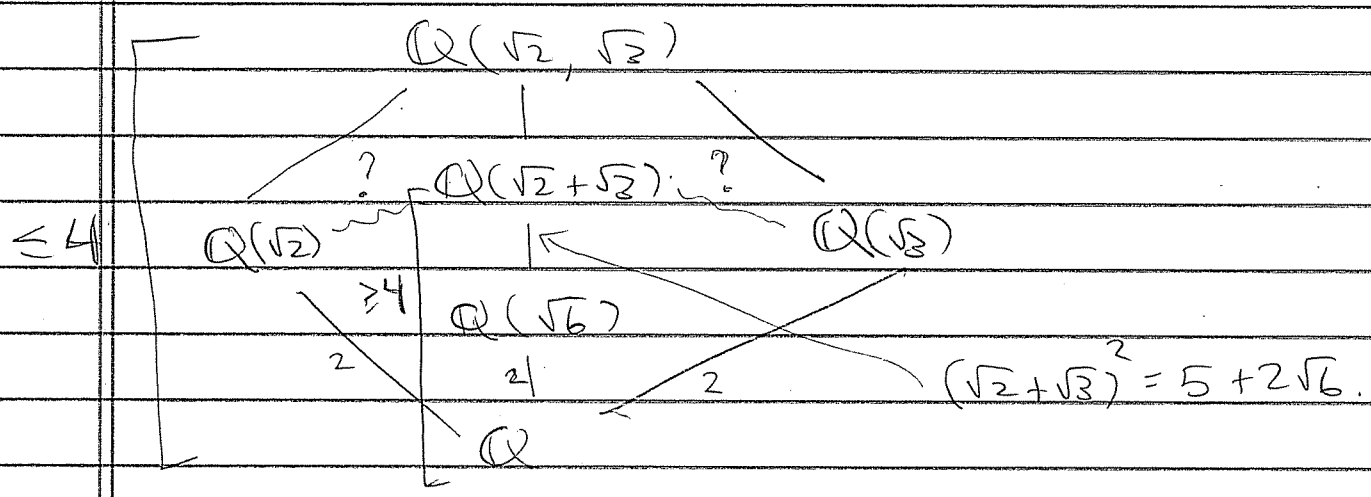
$$F(\alpha_1, \ldots, \alpha_n) = \bigcap_{F \cup \{\alpha_1, \ldots, \alpha_n\} \subseteq E \subseteq K} E.$$



Q: $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$?

Claim: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Proof: The following inclusions are easy



Note:

(1) $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ span $\mathbb{Q}(\sqrt{2},\sqrt{3})$ hence $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] \leq 4$.

(2) $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{6})$ since

$\sqrt{2}+\sqrt{3} = a+b\sqrt{6}$.

$5+2\sqrt{6} = a^2+6b^2+2ab\sqrt{6}$

$\Rightarrow \sqrt{6} \in \mathbb{Q}$ ✗

Hence $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \geq 4$.

(1)+(2) $\Rightarrow$ $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ ∎

Corollary: $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

[You will give an explicit proof on HW 4.]

General fact

Primitive Element Theorem (Steinitz, 1910).
If $\mathbb{Q} \subseteq F \subseteq K$ with $\alpha, \beta \in K$ alg. over F, then

$$F(\alpha, \beta) = F(\gamma)$$

for some $\gamma \in K$. [Note that $\mathbb{Q} \subseteq F$, i.e. F must have "characteristic 0"]

DEF: Given $f(x) \in F[x]$ we say that $K \supseteq F$ is a splitting field for f/F if

- f splits over K.
- If $F \subseteq E \subsetneq K$ then f does NOT split over E.

(K is minimal).

The Fundamental Theorem of Field Theory (Kronecker, 1887).

Given $f(x) \in F[x]$ $\exists$ field extension $K \supseteq F$ in which f has a root.

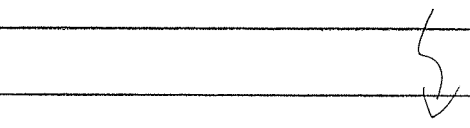
Proof: Let $p(x)$ be an irred factor of $f(x)$ and consider the field $K = F[x]/(p) \supseteq F$. Then $x + (p(x))$ is a root of $f(x) \in K[x]$ because:

$$p(x + (p(x))) = p(x) + (p(x)) = (p(x)) = \text{"0"}.$$

Since $p \mid f$ over K, we get $f(x + (p(x))) = \text{"0"}$. ▨

Corollary: Splitting fields exist.

Proof: Given $f \in F[x]$, Kronecker $\Rightarrow$ $\exists$ $K \supseteq F$ with $a \in K$ and $f(a) = 0 \in K$. Factor Theorem $\Rightarrow$ $f(x) = (x - a)\, g(x)$ in $K[x]$. By induction on degree, $\exists$ field $K' \supseteq K \supseteq F$ such that g and hence f splits over K'.



Let E = intersection of all subfields of K' in which f splits.
Then E is a splitting field for f ▨

Theorem: UNIQUENESS.
Given $f \in F[x]$. If $E \supseteq F$, $E' \supseteq F$ are two splitting fields for f then $\exists$ field isomorphism $E \to E'$ fixing F

Proof omitted.

Hence we can discuss "the" splitting field of $f \in F[x]$ up to isomorphism

Ex. The splitting field of $x^3 - 2 \in \mathbb{Q}[x]$.

$x^3 - 2$ has roots $\sqrt[3]{2}, \omega(\sqrt[3]{2}), \omega^2(\sqrt[3]{2}) \in \mathbb{C}$
where $\omega = e^{2\pi i/3}$.

$$\Rightarrow E = \mathbb{Q}(\sqrt[3]{2}, \omega(\sqrt[3]{2}), \omega^2(\sqrt[3]{2}))$$
$$= \mathbb{Q}(\sqrt[3]{2}, \omega)$$
is the splitting field.

HW 4 due this Fri

Exam 2 Wed Mar 28

Today: Galois.

DEF: Given field F and poly $f(x) \in F[x]$ we say $K \supseteq F$ is a splitting field for f if

- $f(x)$ splits in $K[x]$
- If $F \subseteq E \subseteq K$ and $f(x)$ splits in $E[x]$ then $E = K$. (K is MINIMAL)

Kronecker's Theorem (1889).
Given $f(x) \in F[x]$, $\exists$ field $E \supseteq F$ in which f has a root

Proof: Let $p(x) \mid f(x)$ be a proper factor in $F[x]$ (i.e. $p(x)$ is irred / F).
Then f has a root in the field

$$F[x]/(p) \supseteq F.$$

The root is $x + (p)$. ∎

Corollary: Every $f(x) \in F[x]$ has a splitting field.

Proof: Induction on $\deg(f)$ ☑

Theorem (uniqueness): If E, E' are splitting fields for $f(x) \in F[x]$ then $\exists$ field isomorphism $\varphi: E \to E'$ s.t.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{id.} & F \end{array}$$ commutes.

i.e. $\varphi|_F = id.$ i.e. $\varphi(a) = a \quad \forall\, a \in F$.

Proof omitted.

So we can discuss THE splitting field of f/F.

Remark: If $\mathbb{Q} \subseteq F$ (say "char$(F) = 0$") we don't have to be so careful.

Fundamental Theorem of Algebra
$\Rightarrow$ every polynomial $f(x) \in \mathbb{Q}[x]$ splits over $\mathbb{C}$. Hence we can identify the splitting field of $f(x)$ with a subfield of $\mathbb{C}$.

$$\mathbb{Q} \subseteq F \subseteq K \subseteq \mathbb{C}$$

$\uparrow$
the splitting field for some $f(x) \in F[x]$.

This makes things much more concrete.

☆ Useful fact: Suppose $f(x) \in F[x]$ with $F \supseteq \mathbb{Q}$ has roots $a_1, a_2, \ldots, a_n \in \mathbb{C}$ (with possible repetition). Then the splitting field of $f(x)$ is

$$F \subseteq F(a_1, a_2, \ldots, a_n) \subseteq \mathbb{C}$$

$\uparrow$
the smallest subfield of $\mathbb{C}$ containing $F \cup \{a_1, \ldots, a_n\}$ ///

Ex. The splitting field of $x^2 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) \subseteq \mathbb{C}$.

Ex The splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(a_1, a_2, a_3)$ where

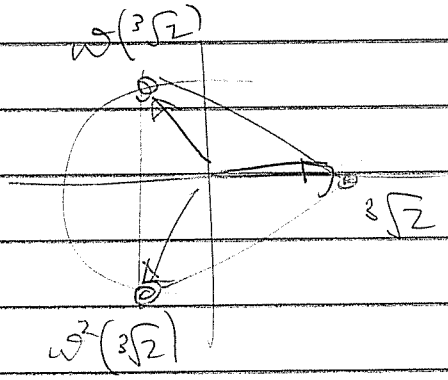
$a_1 = \sqrt[3]{2}$ (real cube root)

$a_2 = \omega(\sqrt[3]{2})$

$a_3 = \omega^2(\sqrt[3]{2})$

$\left[\omega = e^{2\pi i/3}\right]$

Picture:



$x^3 - 1 = (x - a_1)(x - a_2)(x - a_3)$

Claim: $\mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

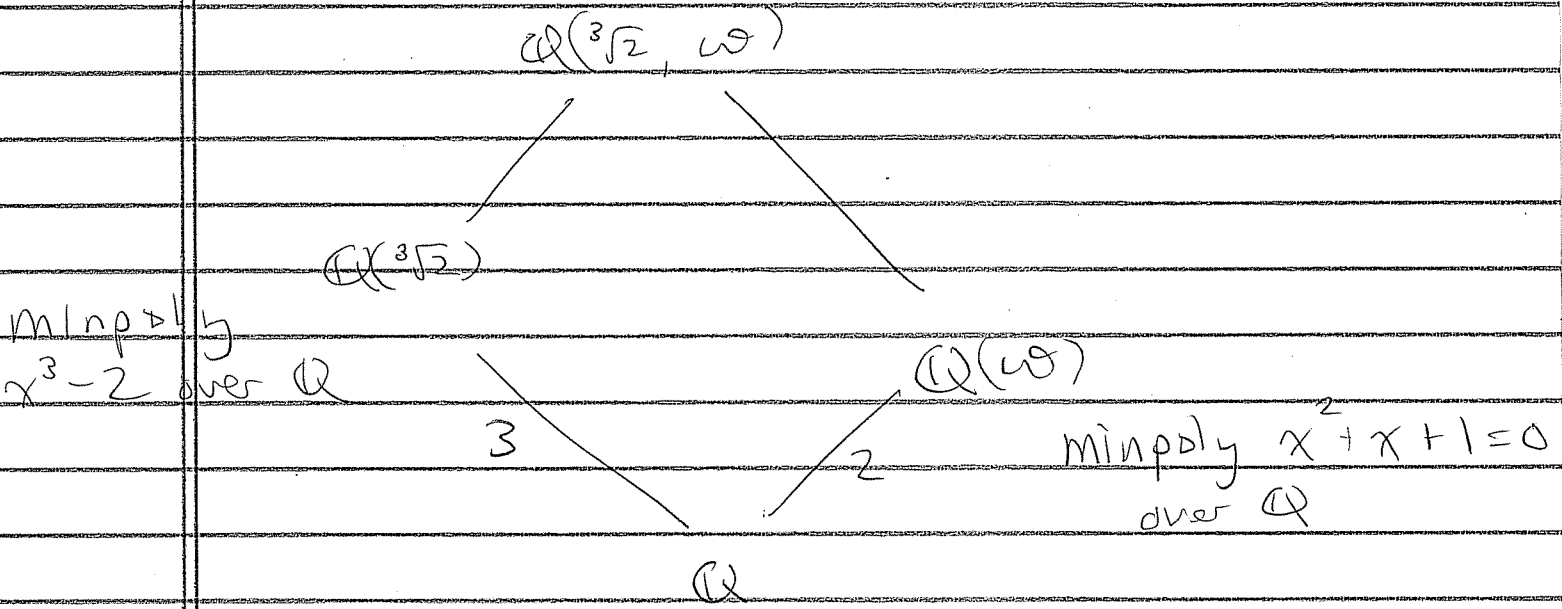
Proof: $a_1, a_2, a_3 \in \mathbb{Q}(\sqrt[3]{2}, \omega)$ (easy)

$\Rightarrow \mathbb{Q}(a_1, a_2, a_3) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Conversely, $\sqrt[3]{2}$, $\omega = \frac{a_2}{a_1} \in \mathbb{Q}(a_1, a_2, a_3)$

$\Rightarrow \mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{Q}(a_1, a_2, a_3)$ //

Q: $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = ?$



Tower Law $\Rightarrow$ 2 & 3 divide $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$

$\Rightarrow$ 6 divides $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$

But $1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega(\sqrt[3]{2}), \omega(\sqrt[3]{2})^2$

spans $\mathbb{Q}(\sqrt[3]{2}, \omega)$ over $\mathbb{Q}$

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] \leq 6.$

Conclusion: $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6.$

Question: $\exists\, \alpha \in \mathbb{C}$ such that

$\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\alpha)$? ?

Ex. splitting field of $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$ is

$$\mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

↑ proved before.

In general we have

Primitive Element Theorem (Steinitz, 1910).
If $\mathbb{Q} \leq F \leq K$ ("char(F) = 0")
with $a, b \in K$ alg. over F then

$$F(a,b) = F(c)$$

for some $c \in K$. (Proof omitted.)

Corollary: Given $\mathbb{Q} \leq F$, let $F \leq K$ be the splitting field of $f(x) \in F[x]$. Say f has roots $a_1, a_2, \ldots, a_n \in \mathbb{C}$. Then

$$K = F(a_1, a_2, \ldots, a_n) = F(c) \leq \mathbb{C}$$

↑ induction using Steinitz.

HW due Fri

Exam 2 next Wed.

Today: Galois' big idea.

Recall: Given fields $\mathbb{Q} \leq F$ and polynomial $f(x) \in F[x]$, say f has roots $a_1, a_2, \ldots, a_n \in \mathbb{C}$ ($\exists$ by FTA). Then K where

$$F \leq K = F(a_1, \ldots, a_n) \leq \mathbb{C}$$

is called the splitting Field of f / F.

By Steinitz' Primitive Element Theorem we can write

$$K = F(a_1, a_2, \ldots, a_n) = F(c) = \mathbb{C}.$$

for some $c \in \mathbb{C}$. (called a primitive element of K).

☆ BIG DEFINITION:

Given a field extension $F \subseteq K$, we define the Galois group

$$\mathrm{Gal}(K/F) := \{ \text{field isomorphisms } K \to K \text{ that fix } F \text{ pointwise} \}$$

i.e. φ such that

$$\begin{array}{ccc} K & \xrightarrow{\varphi}_{\sim} & K \\ \uparrow & & \uparrow \\ F & \xrightarrow{id} & F \end{array}$$

$\mathrm{Gal}(K/F)$ is a group under composition of maps.

☆ Galois' BIG IDEA:

If K is the split. field for $f(x) \in F[x]$. then $\mathrm{Gal}(K/F)$ encodes the relationship

$$F \longleftrightarrow K.$$

coeffs. of f $\longleftrightarrow$ roots of f

?

So what? Recall: If α, β are the roots of $ax^2 + bx + c$, then

$$x^2 + \frac{b}{a}x + \frac{c}{a} = (x-\alpha)(x-\beta)$$
$$= x^2 - (\alpha+\beta)x + \alpha\beta.$$

So roots $\rightsquigarrow$ coeffs is easy.

$$b/a = -(\alpha+\beta).$$
$$c/a = \alpha\beta.$$

How to go coeffs $\rightsquigarrow$ roots?

$$\alpha = \left(-b + \sqrt{b^2-4ac}\right)/2a$$
$$\beta = \left(-b - \sqrt{b^2-4ac}\right)/2a$$

This is famous.

Goal: Do the same for all polynomials.

i.e. Given $a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, find a "formula" for the α_i in terms of the a_i and "simple algebraic operations".

History:

Degree 2 - ancient
Degree 3 - Cardano et al. 1540's Italy.
Degree 4 - Cardano's student Ferrari (1545)
STUCK!

Cardano's cubic formula in modern language. (Lagrange)

Let $x^3 - e_1 x^2 + e_2 x - e_3$ have roots r_1, r_2, r_3 and define

$$\left.\begin{aligned} s_1 &= r_1 + r_2 + r_3 \\ s_2 &= r_1 + \omega r_2 + \omega^2 r_3 \\ s_3 &= r_1 + \omega^2 r_2 + \omega r_3 \end{aligned}\right\} \quad \omega = e^{2\pi i/3}.$$

This can be inverted.

$$\begin{aligned} r_1 &= 1/3\,(s_1 + s_2 + s_3) \\ r_2 &= 1/3\,(s_1 + \omega^2 s_2 + \omega s_3) \\ r_3 &= 1/3\,(s_1 + \omega s_2 + \omega^2 s_3). \end{aligned}$$

New Goal: Solve for s_1, s_2, s_3 in terms of e_1, e_2, e_3.

$s_1 = e_1$ ✓ easy.

USEFUL FACT (Newton): Any polynomial in r_1, r_2, r_3 that is symmetric under permuting r_i's can be written as a polynomial in e_1, e_2, e_3.

Note that $A = s_2^3 + s_3^3$

$B = s_2^3 s_3^3$

are symmetric in r_1, r_2, r_3.

Newton $\Longrightarrow$ $A = 2e_1^3 - 9e_1e_2 + 27e_3$.

$B = (e_1^2 - 3e_2^2)^3$

Finally note that s_2^3, s_3^3 are roots of

$(x - s_2^3)(x - s_3^3) = x^2 - (s_2^3 + s_3^3)x + s_2^3 s_3^3$

$= x^2 - Ax + B$.

$\Longrightarrow$ $s_2^3, s_3^3 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B})$ Quad Formula.

$\Longrightarrow$ $s_2, s_3 = \sqrt[3]{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}$

= "radical expression" in e_1, e_2, e_3 ✓ ☺

History:

1824: Abel (1802-1829) proved you can't "do this" for the quintic

~1830: Galois (1811-1831) gave the correct proof.

Theorem: Let $f(x) \in F[x]$ have splitting field K and consider the group $G = Gal(K/F)$. Then

f is "solvable by radicals"

$\Updownarrow$

$\exists$ chain of normal subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

(say G is "solvable")

with G_i/G_{i-1} abelian $\forall\, i$.

In the process, Galois invented the concept of a "group".

Review for Exam 2

Theme: Polynomials in 1 variable.

Let R be comm. ring with 1.

Theorem: Consider an ideal $I \subsetneq R$.

(1) R/I field $\iff$ I is maximal

(2) R/I domain $\iff$ I is prime.

Proof of (2): Recall ring R/I has $1_{R/I} = 1 + I$ and $0_{R/I} = 0 + I = I$.

Sp. I is prime and consider $a+I, b+I \neq I$ (i.e. $a \notin I$, $b \notin I$). Then I prime $\Rightarrow ab \notin I$ $\Rightarrow (a+I)(b+I) = ab + I \neq I$. ///

Conversely, sp. R/I a domain. Consider $a, b \in R$ with $ab \in I$ (i.e. $ab + I = I$). Then R/I domain $(a+I)(b+I) = I \Rightarrow a+I = I$ (i.e. $a \in I$) OR $b+I = I$ (i.e. $b \in I$) ///

Given any ring R define

$$R[x] := \left\{ \sum_{i \geq 0} a_i x^i \;:\; a_i \in R,\ a_i = 0 \text{ almost always} \right\}$$

x is just a formal placeholder ("variable")

Now let R be a domain.

FACTS:

① $R[x]$ is a domain with $\deg(fg) = \deg(f) + \deg(g)$ and $(R[x])^\times = R^\times$
(Think: what does $R \subseteq R[x]$ mean?).

② Given $f, g \in R[x]$, g monic, $\exists\, q, r \in R[x]$

$$f = qg + r, \quad \deg(r) < \deg(g) \text{ or } r = 0.$$

Proof: long division. ☒

(2) Cor: For F a field, $F[x]$ is a Euclidean Domain ($\Rightarrow$ PID $\Rightarrow$ UFD).

(3) Cor: Given $f(x) \in R[x]$, $\alpha \in R$.

"$f(\alpha) = 0$" $\iff$ $(x - \alpha) \mid f(x)$ in $R[x]$.

Say α is root of multiplicity k if $k \in \mathbb{N}$ largest such that $(x-\alpha)^k \mid f(x)$.

(4) Cor: Given $\deg(f) = n$, then f has $\leq n$ roots counting multiplicity.

Issue: What does "$f(\alpha)$" mean?

Consider $R \subseteq S$. Then $\forall \alpha \in S$ $\exists!$ ring hom $\varphi_\alpha : R[x] \to S$

$$\begin{cases} x \longmapsto \alpha \\ a \longmapsto a \quad \forall a \in R. \end{cases}$$

Notation: $f(\alpha) := \varphi_\alpha(f(x)) \in S$.

DEF: $R[\alpha] := \operatorname{im} \varphi_\alpha \subseteq S$

FACT: $R[\alpha]$ is the smallest subring of S containing $R \cup \{\alpha\}$.

SAY: $R[\alpha]$ = "R adjoin α".

1st Iso. Thm:

$$R[x] / \ker \varphi_\alpha \cong \operatorname{im} \varphi_\alpha = R[\alpha] \subseteq S.$$

~~$f(x) + \ker \varphi \longmapsto f(\alpha)$.~~

Now let F be a field, so $F[x]$ is PID.

Given $F \subseteq K$ with $\alpha \in K$ alg. / F we have

$$F[\alpha] = \operatorname{im} \varphi_\alpha \cong F[x]/\ker\varphi_\alpha = F[x]/(f_\alpha(x))$$

for unique, monic $f_\alpha \in F[x]$.

FACTS:

(1) $f_\alpha(x)$ is irreducible.

Proof: If $f_\alpha(x) = g(x)h(x)$ then
$g(\alpha)h(\alpha) = f_\alpha(\alpha) = 0 \Rightarrow$ WLOG $g(\alpha) = 0$
$\Rightarrow g \in \ker\varphi_\alpha = (f_\alpha) \Rightarrow (g) = (f_\alpha)$. ///

(2) Cor: $F[\alpha] = F(\alpha) =$ the smallest subfield of K containing $F \cup \{\alpha\}$.

(3) If $\deg(f_\alpha)$ then $F(\alpha)$ is a vector space over F with basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

i.e. $[F(\alpha) : F] = \dim_F F(\alpha) = \deg(f_\alpha)$.

Tower Law: Given fields $F \subseteq K \subseteq L$,

$$[L:F] = [L:K] \cdot [K:F]$$

Proof: If $L:K$ has basis $\alpha_1, \dots, \alpha_m$
and $K:F$ has basis $\beta_1, \dots, \beta_n$

Then $L:F$ has basis $\{\alpha_i \beta_j\}_{i,j}$

Kronecker's Theorem (1887).

Given field F and $f(x) \in F[x]$, $\deg(f) \geq 1$,
$\exists$ field $K \supseteq F$ and $\alpha \in K$ with $f(\alpha) = 0$.

i.e. $\varphi_\alpha : F[x] \longrightarrow K$.
$f(x) \longmapsto 0$

Proof: sp. $f(x) = g(x)p(x)$, p irred.

Take. $K = F[x]/(p(x))$, $\alpha = x + (p(x))$.

$f(x) \longmapsto f(x) + (p(x))$

$F[x] \longrightarrow F[x]/(p(x))$ K

$\cup$ $\cup$ field extension. $\cup$

$F \xrightarrow{\sim} F$ F

$a \longmapsto a + (p(x))$

K

$\varphi_{x+p(x)} : F[x] \longrightarrow F[x]/(p(x))$.

α

DEF: $\begin{cases} x \longmapsto x + (p(x)). \\ a \longmapsto a + (p(x)). \end{cases}$

Then $f(x) \longmapsto f(x) + (p(x))$.

But since $f(x) = g(x)p(x)$ we have

$f(x) \longmapsto g(x)p(x) + (p(x))$

$= (p(x)) =$ "0" in $\frac{F[x]}{(p(x))}$.

So by definition:

"$f(x + (p(x))) = 0$".

this is a root of f in an extension field.

Cor: Every poly has a splitting field.

Proof: Induction on degree.

Discuss the FTA.