# Background from Algebra 2

- finite fields, field extensions
- algebraic extensions
- transcendental extensions
- splitting fields
- Ruler-and-compass constructions

- polynomial irreducibility (Eisenstein?)
- reduction mod $n$?

═══ Chapter 5 of Hungerford ═══

## Definition

If $K \subset F$ are fields, then $F$ is called a field extension or extension of $K$. Furthermore, $F$ is a vector space over $K$ and the dimension of this vector space will be denoted $[F:K]$.

---

Why? By definition, $(F,+)$ is an abelian group, and distributivity/associativity holds for multiplication by elements of $F$, so certainly for elements of $K$, too. This proves it.

---

**Theorem**: Let $F$ be an extension of $E$ which is an extension of $K$. Then $(F \supseteq E \supseteq K)$

$$[F:K] = [F:E][E:K].$$

**Proof**: Choose bases $\alpha = \{\alpha_1, \ldots, \alpha_m\}$ and $\beta = \{\beta_1, \ldots, \beta_n\}$ of $F/E$ and $E/K$ resp.

Then $\gamma = \{\alpha_i \beta_j \mid 1 \le i \le m,\ 1 \le j \le n\}$

is a basis of $F/K$. To see it spans, given $f \in F$ write

$$f = \sum_{i=1}^{m} b_i \alpha_i \quad \text{since } \alpha_i \text{ are a basis for } F/E$$

where $b_i \in E$.

Then for each $b_i$ write $b_i = \sum_{j=1}^{n} c_j \beta_j$ where $c_j \in K$.

Then $f = \sum_{i=1}^{m} \left( \sum_{j=1}^{n} c_{ij} \beta_j \right) \alpha_i$, then multiply it out to get $f$ in terms of products $\beta_j \alpha_i$.

On the other hand if $\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij}\, \alpha_i \beta_j = 0$

$$\iff \sum_{j=1}^{n} c_{ij} \beta_j = 0 \ \forall i \quad \text{since } \{\alpha_1, \ldots, \alpha_m\} \text{ a basis}$$

$$\iff \forall i, j \quad c_{ij} = 0 \quad \text{since } \{\beta_1, \ldots, \beta_m\} \text{ a basis.}$$

---

<u>Terminology</u>: If $F$ is a field and $X \subset F$ is a set, then the subfield <u>generated by $X$</u> is the intersection of all subfields of $F$ containing $X$.

If $F$ is an extension of $K$ and $X \subset F$ then the subfield generated by $K \cup X$ is called <u>the subfield generated by $X$ over $K$</u> and is written $K(X)$. If $X = \{u_1, \dots, u_n\}$ then $K(X)$ is written $K(u_1, \dots, u_n)$. If $X = \{u\}$ then $K(u)$ is called a <u>simple extension</u> of $K$.

If, instead of taking the intersection of all sub<u>fields</u> of $F$ containing $X$ we take the intersection of all <u>subrings</u> then it's called the sub<u>ring</u> generated by $X$. Our notations change from $K(X)$, $K(u_1, \dots, u_n)$ and $K(u)$ to $K[X]$, $K[u_1, \dots, u_n]$ and $K[u]$.

<u>Theorem</u>: Suppose $K \subset F$ are fields and $u, u_i \in F$ and $X \subset F$. Then:

(i) $K[u]$ consists of elements of the form $f(u)$ where $f$ is a polynomial with coefficients in $K$.

(ii) The subring $K[u_1, \dots, u_m]$ similarly consists of $g(u_1, \dots, u_m)$ where $g$ is a polynomial over $K$ with $m$ indeterminates.

(iii) The subring $K[X]$ is all polynomial elements $h(u_1, \ldots, u_n)$ for some $n \in \mathbb{N}$ and $u_i \in X$.

(iv) The subfield $K(u)$ is all elements of $F$ of the form $f(u) g^{-1}(u) =: \dfrac{f(u)}{g(u)}$ where $f, g \in K[x]$.

(v) The subfield $K(u_1, \ldots, u_m)$ is all elements

$$\frac{f(u_1, \ldots, u_m)}{g(u_1, \ldots, u_m)} := f(u_1, \ldots, u_m)\, g(u_1, \ldots, u_m)^{-1}, \; f, g \in K[x_1, \ldots, x_m].$$

(vi) The subfield $K(X)$ is similarly quotients of the elements from (iii).

(vii) For each $f \in K[X]$ (or $K(X)$) there is a finite subset $X' \subset X$ such that $f \in K[X'] \subset K[X]$ ($f \in K(X') \subset K(X)$).

---

<u>Terminology</u>: If $L, M \subset F$ are subfields, then $LM$ is the <u>composite</u> of $L$ and $M$ and is the subfield generated by $L \cup M$.

<u>Definition</u>: Let $K \subseteq F$ be fields. An element $u \in F$ is algebraic over $K$ provided that $\exists\, f(x) \in K[x]$ such that $f(u) = 0$ ($f \neq 0$).

If no such $f$ exists, then $u$ is transcendental over $K$. The extension $F/K$ is algebraic if every element of $F$ is algebraic over $K$, and transcendental otherwise.

Remarks: Every element $u$ of $K$ is algebraic over $K$, since it's a root of $x-u \in K[x]$.

Example: The polynomial ring $K[x_1, \dots, x_n]$, $K$ a field, sits inside of a larger field ~~as~~ called the field of fractions of $K[x_1, \dots, x_n]$. We use $\frac{f}{g}$ to denote the equivalence class of pairs $(f,g)$ where $(f,g) \sim (h,k)$ iff $fk = hg$. With the usual fraction addition/mult, this is a field containing $K[x_1, \dots, x_n]$. So we get

$$K \subset K[x_1, \dots, x_n] \subset \underbrace{K(x_1, \dots, x_n)}_{\text{field of fractions.}}$$

Then every element of $K(x_1, \dots, x_n) \setminus K$ is transcendental over $K$. (Exercise on next asst).

Theorem: Suppose that $K \subseteq F$ are fields and that $u \in F$ is transcendental over $K$. Then there is a field isomorphism $\varphi: K(u) \longrightarrow K(x)$ such that $\varphi(k) = k \ \forall k \in K$. (Here, $K(x)$ is the field of rational functions).

Proof: Given $f, g$ nonzero polynomials in $K[x]$, we know $f(u)$ and $g(u)$ are both nonzero. Thus the map $\varphi: K(x) \longrightarrow K(u)$ given by $\varphi\left(\frac{f}{g}\right) = \frac{f(u)}{g(u)} = f(u)g(u)^{-1}$ is a well-defined field homomorphism, and it is the identity on $K$ since evaluating a constant $k \in K$ at $u$ yields $k$ again.

But now $\varphi$ is clearly an onto homomorphism, since our theorem last day claimed elements of $K(u)$ were exacty of the form $f(u)g(u)^{-1}$. Field homomorphisms are injective, so it's iso.

Lemma: Field homomorphisms are injective

Proof: Suppose $\varphi: F \longrightarrow K$ is a field homo'm, nontrivial. Say $\varphi(a) = \varphi(b)$. Then set $u = a - b$. If $u \neq 0$ then $\varphi(u)\varphi(u^{-1}) = \varphi(uu^{-1}) = \varphi(1) = 1$, but at the same time $\varphi(u) = 0$. So $0 \cdot \varphi(u^{-1}) = 1$, a contradiction.

<u>Moral</u>: When $u \in F \setminus K$ is transcendental over $K$, the extension $K(u)$ is rather uninteresting. What about when $u \in F \setminus K$ is algebraic over $K$?

<u>Theorem 1.6</u>: Suppose that $K \subseteq F$ are fields, and that $u \in F$ is algebraic over $K$. Then:

(i) $K(u) = K[u]$

(ii) $K(u) \simeq K[x]/(f(x))$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by requiring (a) $f(u) = 0$ and (b) for all other $g \in K[x]$, if $g(u) = 0$ then $f$ divides $g$.

(iii) $[K(u) : K] = n$

(iv) $\{1, u, u^2, \dots, u^{n-1}\}$ is a basis for $K(u)$ as a vectorspace over $K$

(v) Every element in $K(u)$ can be written as $\sum_{i=0}^{n-1} a_i u^i$,

<u>Proof</u>: Let us prove (ii). Define ~~f~~ $\varphi : K[x] \longrightarrow K[u]$ to be the surjective! ring homomorphism $\varphi(g) = g(u)$ for all $g \in K[x]$. Since $K[x]$ is a PID, and $\ker \varphi$ is an ideal, we know that $\ker \varphi = (f)$ for some polynomial $f \in K[x]$, with $f(u) = 0$. Since $u$ is algebraic $\ker \varphi$ is nontrivial, ~~and~~ and $f$ has degree $\geq 1$ since $\ker \varphi \neq K[x]$ as $\varphi$

is not the zero homomorphism. Furthermore, we can assume $f$ is monic: If it were not monic, say $f(x)$ has leading coefficient $c$, then $c^{-1}f$ is monic and $(c^{-1}f) = (f) = \ker f$, so we can replace $f$ with $c^{-1}f$. By the first isomorphism theorem:

$$K[x]/(f) = K[x]/\ker\varphi \cong K[u].$$

Next, since $K[u]$ is an integral domain (it's a subring of a field) we know that $(f)$ must be prime. But then $f$ is an irreducible polynomial, which implies $(f)$ is a maximal ideal. So $K[x]/(f)$ is a field, so $K[u] \subset K(u)$ implies $K[u] = K(u)$. So (i) is true.

Last we prove (iv), with (iii) and (v) being more or less immediate consequences.

Every element in $K(u)$ is of the form $g(u)$ for some $g \in K[x]$. Then

$$g = qf + h \text{ where } \deg h < \deg f. \text{ So}$$

$$g(u) = q(u)f(u) + h(u) = 0 + h(u) = a_0 + a_1 u + \dots + a_m u^m$$

with $m < n = \deg f$. Thus $\{1, u, \dots, u^{n-1}\}$ span $K(u)$.

To see linear independences suppose $\sum_{i=0}^{n-1} a_i u^i = 0$ $(a_i \in K)$. Then $g(x) = \sum_{i=0}^{n-1} a_i x^i$ has a root at $u$, but $\deg g = n-1$ is less than $\deg f = n$. But since $g(u) = 0$ must give $f \mid g$, this forces $g = 0$.

<u>Definition</u>: Let $F$ be an extension of $K$, and $u \in F$ algebraic over $K$. The <u>minimal polynomial of $u$</u> is $f$ from the previous theorem. The <u>degree of $u$ over $f$</u> is $\deg f = [K(u) : K]$.

<u>Example</u>: What is $\left[\mathbb{Q}\left(\sqrt{\frac{1+\sqrt{-3}}{2}}\right) : \mathbb{Q}\right]$ ?

<u>Solution</u>: Let $\alpha = \sqrt{\frac{1+\sqrt{-3}}{2}}$. Then

$$\alpha^2 = \frac{1+\sqrt{-3}}{2}$$

$$\Rightarrow 2\alpha^2 = 1 + \sqrt{-3}$$

$$\Rightarrow 2\alpha^2 - 1 = \sqrt{-3}$$

$$\Rightarrow (2\alpha^2 - 1)^2 = -3$$

$$\Rightarrow 4\alpha^4 - 4\alpha^2 + 4 = 0.$$

remove 4's, get $f(x) = x^4 - x^2 + 1$.

Set $f(x) = \cancel{4}x^4 - \cancel{4}x^2 + \cancel{4}$. Then via the quadratic formula, we know $f(x)$ has four roots:

$$\alpha_1 = \sqrt{\frac{1+\sqrt{-3}}{2}}, \quad \alpha_2 = -\alpha_1, \quad \alpha_3 = \sqrt{\frac{1-\sqrt{-3}}{2}}, \quad \alpha_4 = -\alpha_3,$$

none of which are in $\mathbb{Q}$. Thus $f(x)$ does not factor as a cubic times a linear factor.

(Alternatively: The rational root test implies $f(x)$ has no roots in $\mathbb{Q}$ since $\pm 1$ are not roots of $f(x)$)

Aside

Rational root test: If $a_i \in \mathbb{Z}$ and $a_n x^n + \dots + a_1 x + a_0 = 0$, then $x = \frac{p}{q}$ is a solution means $p, q$ must satisfy:

- $p$ divides $a_0$
- $q$ divides $a_n$

So here, our polynomial is monic with constant term 1

$$\Rightarrow p, q = \pm 1.$$

Next suppose $f(x)$ factors as two quadratics. Then

$$f(x) = (x^2 + ax + b)(x^2 - ax + b)$$

(this is because the coeffs of $x^3$ and $x$ in $f(x)$ are zero).

$$\Rightarrow x^4 - x + 1 = x^4 + (2b - a^2)x^2 + b^2.$$

$$\Rightarrow b = \pm 1 \text{ and } 2b - a^2 = -1.$$

$$\Rightarrow \pm 2 - a^2 = -1.$$

If $-2 - a^2 = -1$

$\Rightarrow -a^2 = 1$

$\Rightarrow$ no solution in $\mathbb{Q}$

$2 - a^2 = -1$

$\Rightarrow -a^2 = -3$

$\Rightarrow$ no solution in $\mathbb{Q}$.

Thus $f(x)$ is irreducible over $\mathbb{Q}$. So $f(x)$ is the minimal polynomial of $\alpha$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$.

__Example__: Consider $x^3-3x-1 \in \mathbb{Q}[x]$. This polynomial is irreducible over $\mathbb{Q}$ since reduction of coeffs mod 2 gives $x^3-x-1$, which has no roots in $\mathbb{Z}_2$ and is thus irreducible in $\mathbb{Z}_2[x]$ — therefore, it's irreducible in $\mathbb{Z}[x]$ and hence $\mathbb{Q}[x]$. It does, however, have at least one real root $u \in \mathbb{R}$.

~~Thus~~

By the previous theorem, then, $[\mathbb{Q}(u):\mathbb{Q}] = \deg(x^3-3x-1) = 3$, and so $\{1, u, u^2\}$ is a basis for $\mathbb{Q}(u)$ over $\mathbb{Q}$.

How do we use this to do computations in $\mathbb{Q}(u)$? Since $u$ is algebraic, $\mathbb{Q}(u) = \mathbb{Q}[u]$ and so every element in $\mathbb{Q}(u)$ can be written as

$$\sum_{i=1}^{n} a_i u^i \quad \text{for some } a_i \in \mathbb{Q} \text{ and } n \in \mathbb{N}.$$

Consider, for example, $u^4+2u^3+3 \in \mathbb{Q}[u]$. Under the isomorphism $\mathbb{Q}[u] \simeq \mathbb{Q}[x]/(x^3-3x-1)$ this maps to the coset $x^4+2x^3+3+\underbrace{(x^3-3x-1)}_{= I}$. Then polynomial long division in $\mathbb{Q}[x]$ yields

$$\begin{array}{r l}
 & x+2 \\
x^3-3x-1 \,\big) & x^4+2x^3+0x^2+0x+3 \\
 & -(x^4 \qquad\; -3x^2-x) \\
\hline
 & 0+2x^3+3x^2+x+3 \\
 & -(2x^3-0x^2-6x-2) \\
\hline
 & \qquad 3x^2+7x+5
\end{array}$$

$$\text{So } x^4+2x^3+3+\underbrace{(x^3-3x-1)}_{\text{ideal}}\overset{I}{}$$

$$= 3x^2+7x+5+(x+2)(x^3-3x-1)+\overbrace{(x^3-3x-1)}^{\text{ideal}}_{=I}$$

$$= 3x^2+7x+5+I$$

Then passing from $\mathbb{Q}[x]/(x^3-3x-1)$ to $\mathbb{Q}[u]$ via the isomorphism again, we arrive at $3u^2+7u+5$.

<u>What have we done here?</u>

We've established that $u^4+2u^3+3 = 3u^2+7u+5$ in $\mathbb{Q}[u]$, meaning that relative to the basis $\{1, u, u^2\}$ the element $u^4+2u^3+3$ is written as $5+7u+3u^2$ or $\begin{bmatrix}5\\7\\3\end{bmatrix}$.

Second computation: But $\mathbb{Q}[u] = \mathbb{Q}(u)$ is a <u>field</u>, so elements like $u^4+2u^3+3$ have inverses! What is the inverse of $u^4+2u^3+3$?

We pass to $\mathbb{Q}[x]/(x^3-3x-1)$ via the isomorphism above, arriving at the polynomial $x^4+2x^3+3+I$

$$= 3x^2+7x+5+I.$$

Now in $\mathbb{Q}[x]$, since $x^3-3x-1$ is irreducible the polynomials $3x^2+7x+5$ and $x^3-3x-1$ are relatively prime, so $\exists\, g(x), h(x)$ with

$$(3x^2+7x+5)g(x) + (x^3-3x-1)h(x) = 1.$$

$$\Rightarrow (3x^2+7x+5+I)(g(x)+I) = 1+I,$$

so $g(x)$ is the inverse in $\mathbb{Q}[x]/(x^3-3x-1) \simeq \mathbb{Q}[u]$.

The Euclidean Algorithm gives

$$g(x) = \frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}, \text{ so}$$

$\frac{7}{111}u^2 - \frac{26}{111}u + \frac{28}{111}$ is the inverse of $u^4 + 2u^3 + 3$

in $\mathbb{Q}(u)$.