Field Theory

Book 2

Claim: $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ i.e. $\sqrt{3} = a + b\sqrt{2}$ has no solution with $a, b \in \mathbb{Q}$.

Suppose $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ so $2ab\sqrt{2} = 3 - a^2 - 2b^2$.

If $ab \neq 0$ then $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$, a contradiction.

If $b = 0$ then $0 = 3 - a^2$ so $a^2 = 3$, $a = \pm\sqrt{3} \notin \mathbb{Q}$, a contradiction.

If $a = 0$ then $0 = 3 - 2b^2$ so $2b^2 = 3$, $4b^2 = 6$, $2b = \pm\sqrt{6} \notin \mathbb{Q}$, a contradiction. □

So $1, \sqrt{2}, \sqrt{3} \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$.

- $1 \neq 0$
- $\sqrt{2} \neq$ scalar multiple of 1. ($\sqrt{2} \notin \mathbb{Q}$ by Euclid
- $\sqrt{3} \neq$ linear combination of $1, \sqrt{2}$. (proved above)

$\sqrt{8} = 2\sqrt{2}$

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23}, \ldots$ are linearly independent.

$[\mathbb{R} : \mathbb{Q}] = \infty$ (in fact uncountable)

Also $1, \pi, \pi^2, \pi^3, \ldots$ are linearly independent over $\mathbb{Q}$. (since π is transcendental).

An extension $E \supseteq F$ is finite if $[E : F] < \infty$, i.e. $[E : F] = n$ is a positive integer.

eg. $\mathbb{C} \supseteq \mathbb{R}$ is a quadratic extension, hence finite. $[\mathbb{C} : \mathbb{R}] = 2$.

A finite extension of $\mathbb{Q}$ i.e. $E \supseteq \mathbb{Q}$ with $[E : \mathbb{Q}] = n$, a positive integer, is called a number field (or algebraic number field). Here every element $\alpha \in E$ is algebraic over $\mathbb{Q}$. Why?

$1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ vectors in an n-dimensional vector space $E \supseteq \mathbb{Q}$ so this list is linearly dependent i.e. $a_0 1 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$ for some $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, not all zero, i.e. α is a root of some nonzero polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Q}[x]$.

If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ then the degree of $f(x)$, denoted $\deg f(x)$, is the largest d such that $a_d \neq 0$.

$\deg(3x^2+5x+7) = 2$

$\deg(0x^2+5x+7) = \deg(5x+7) = 1$

$\deg(7) = \deg(7x^0) = 0$

$\deg 0$ is sometimes left undefined (not 0) or $\deg 0 = -\infty$.

$\deg\left[(3x^2+5x+7)(x^3-4x-11)\right] = \deg(3x^5+\cdots-77) = 5$

$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$.

If $g(x) = x^3-4x-11$ then $0g(x) = 0$

$\deg(0g(x)) = \deg 0$

$\deg 0 + \deg g(x) = \deg 0 + 3$.

$\deg 0 = (\deg 0) + 3$.

There is no integer value for $\deg 0$ that satisfies this.
(We don't choose $+\infty$; we choose $-\infty$.)

Let $\alpha \in \mathbb{C}$. If α is the root of some nonzero poly. $f(x) \in \mathbb{Q}[x]$ (i.e. $f(\alpha) = 0$) then α is algebraic of degree n where n is the smallest degree of any such polynomial $f(x)$. In this case, the smallest degree monic polynomial having α as a root is the minimal polynomial of α (over $\mathbb{Q}$).

eg. $\sqrt{14}$ is algebraic of degree 2 with min. poly. $x^2-14 \in \mathbb{Q}[x]$.

Look at powers $1, \alpha, \alpha^2, \alpha^3, \ldots$ $\alpha = \sqrt{14} \Rightarrow$ $1, \alpha$ lin. indep.

$1, \alpha, \alpha^2$ lin. dep $\alpha^2 = 0\cdot\alpha + 14\cdot 1$

$\alpha = \sqrt{2}+\sqrt{5}$ is algebraic of degree 4 with min. poly. x^4-10x^2+1. Why is $\alpha = \sqrt{2}+\sqrt{5}$ not a root of any smaller degree poly. with rational coefficients?

If $m(x) = x^4 - 10x^2 + 1 = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Q}[x]$ then one of $f(x), g(x)$ is a (nonzero) constant polynomial.
Assuming we start with a monic poly. with integer coefficients, it suffices to check that there is no nontrivial factorization over $\mathbb{Z}[x]$.

If $x^4 - 10x^2 + 1 = f(x)g(x)$, $f(x), g(x) \in \mathbb{Z}[x]$, neither $f(x)$ nor $g(x)$ is constant then either

(i) $\deg f(x) = 1$, $\deg g(x) = 3$; or

(ii) $\deg f(x) = \deg g(x) = 2$.

(The case $\deg f(x) = 3$, $\deg g(x) = 1$ is essentially case (i)).

In both cases we obtain a contradiction.

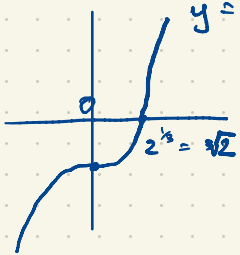
In case (i), $x^4 - 10x^2 + 1 = (x+a)(x^3 + bx^2 + cx + d)$, $ad = 1$, $a = d = \pm 1$.
In this case $m(x)$ has ± 1 as a root but $m(1) = -8 = m(-1)$, a contradiction.

In case (ii), $m(x) = x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c)$, $a, b, c \in \mathbb{Z}$ (since there is no x^3 term on the left).
Once again, $bc = 1$ so $b = c = \pm 1$. Now
$m(x) = x^4 - 10x^2 + 1 = (x^2 + ax \pm 1)(x^2 - ax \pm 1)$. Comparing x^2 terms on both sides,
$-10 = \pm 2 - a^2$ i.e. $a^2 = 10 \pm 2 = 8$ or 12.
This is a final contradiction so $m(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Note: $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}[x]$ as well as in $\mathbb{Q}[x]$: it factors nontrivially as
$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$.
This polynomial has no roots in $\mathbb{Z}$ or in $\mathbb{Q}$ or in $\mathbb{R}$.

$x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$. Every polynomial of degree ≥ 3 in $\mathbb{R}[x]$ is reducible.
$x^4 - 10x^2 + 1 = x^4 + 2x^2 + 1 - 8x^2 = (x^2+1)^2 - (2\sqrt{2}\,x)^2 = (x^2 + 1 + 2\sqrt{2}\,x)(x^2 + 1 - 2\sqrt{2}\,x)$
the polynomial $x - 7$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$. It has a root $7 \in \mathbb{Z}$.
Theorem: If $f(x) \in \mathbb{Z}[x]$ is monic, then $f(x)$ is reducible in $\mathbb{Q}[x]$ iff $f(x)$ is reducible in $\mathbb{Z}[x]$. Assume this, and use it!

For $f(x) \in \mathbb{Q}[x]$ of degree 2 or 3, $f(x)$ is reducible in $\mathbb{Q}[x]$ iff it has a root in $\mathbb{Q}$.
This is not true for $\deg f(x) \geq 4$.
Eg. $f(x) = x^4 + x^2 + 1$ has no roots in $\mathbb{Q}$ but it is reducible in $\mathbb{Q}[x]$
eg. $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ since it has no roots in $\mathbb{Q}$. You need to master this point!
$x^3 - 2$ has no rational roots: it has one real root $2^{1/3} \notin \mathbb{Q}$ essentially by Euclid's argument.



If $\alpha = 2^{1/3} \in \mathbb{Q}$, $\alpha^3 = 2$, write $\alpha = \frac{a}{b}$ with a, b positive integers in lowest terms ($\gcd(a,b) = 1$) then $\frac{a^3}{b^3} = 2$ so $a^3 = 2b^3$ is even so a is even
i.e. $a = 2r$ for some positive integer r. So $8r^3 = 2b^3$ and $b^3 = 4r^3$ is even so b is even i.e. $b = 2s$ for some $s \in \mathbb{Z}$. This contradicts $\gcd(a,b) = 1$.

Now if $x^3 - 2$ is reducible in $\mathbb{Q}[x]$, then $x^3 - 2 = (x+a)(x^2 + bx + c)$, $a, b, c \in \mathbb{Q}$
but then $-a \in \mathbb{Q}$ is a root, contradiction.

For $f(x) \in F[x]$ where F is a field ($f(x)$ is a polynomial in x with coefficients in the field F)
and $r \in F$, we have:

r is a root of $f(x)$	iff	$x - r$ is a {factor / divisor} of $f(x)$ (linear factor i.e. factor of degree 1.)
i.e. $f(r) = 0$		i.e. $f(x) = (x-r)q(x)$, $q(x) \in F[x]$
i.e. r is a "zero" of $f(x)$		

In one direction this "iff" statement is obvious: if $f(x) = (x-r)q(x)$ then $f(r) = (r-r)q(r) = 0$.
What about the converse? By the Division Algorithm, $f(x) = q(x)(x-r) + a(x)$, $\deg a(x) < \deg(x-r)$
($\deg a(x) = 0$ or $-\infty$; $\deg(x-r) = 1$)
If r is a root of $f(x)$ then $f(r) = 0 = q(r)\underbrace{(r-r)}_{0} + a \Rightarrow a = 0$
$\Rightarrow f(x) = q(x)(x-r)$
$a(x) = a$ = constant

We require the Division Algorithm for this.

Review the Division Algorithm for integers $\mathbb{Z}$:

Let $n, d \in \mathbb{Z}$ with $d \geq 1$. (OK for d negative but we cannot use $d = 0$.) In general d won't divide n evenly; there is a remainder.

Theorem There exist unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \leq r < d$.

d = "divisor"
q = "quotient"
r = "remainder"

Eg. $n = 65$, $d = 7$, $65 = 9 \cdot 7 + 2$ $\quad 7 \nmid 65$ $\quad \neq$

$65 = 8 \cdot 7 + 9$

$91 = 13 \cdot 7 + 0$ $\quad 7 \mid 91$.

(quotient, remainder)

$$\begin{array}{r|l} & 9 \\ 7 & 65 \\ & 63 \\ \hline & 2 \end{array}$$

d **divides** n $(d \mid n)$ $\iff$ n is a multiple of d, $n = qd (+0)$ ie. $r = 0$.

Similarly in $F[x]$, F any field. eg. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, ... not $\mathbb{Z}[x]$.

Theorem (Division Algorithm for polynomials) Let F be any field and let $f(x), d(x) \in F[x]$ where $\deg d(x) \geq 1$. Then there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).$$

Eg. $F = \mathbb{Q}$, $f(x) = x^3 - 2x - 3$, $d(x) = x^2 + x + 1$.

$f(x) = x^3 - 2x - 3 = (x-1)(x^2+x+1) + (-2x-2)$

$$\begin{array}{r|l} & x - 1 \\ x^2+x+1 & x^3 \quad -2x - 3 \\ & x^3 + x^2 + x \\ \hline & -x^2 - 3x - 3 \\ & -x^2 - x - 1 \\ \hline & -2x - 2 \end{array}$$

$$x^2+x+1 = \left(-\tfrac{1}{2}x\right)(-2x-2) + (1)$$

$$\begin{array}{r|l} -2x-2 & x^2+x+1 \\ & x^2+x \end{array} \qquad -\tfrac{1}{2}x$$

The Division Algorithm leads to Euclid's Algorithm (for $\mathbb{Z}$, $F[x]$, ... not $\mathbb{Z}[x]$)

$\gcd(100, 27) = 1 = a \cdot 100 + b \cdot 27$ for some $a, b \in \mathbb{Z}$

$100 = 3 \times 27 + 19$

$27 = 1 \times 19 + 8$

$19 = 2 \times 8 + 3$

$8 = 2 \times 3 + 2$

$3 = 1 \times 2 + \boxed{1}$ ← last nonzero remainder

$2 = 2 \times 1 + 0$

$\gcd(100, 27) = 1 = 3 - 2$

$= 3 - (8 - 2 \times 3)$

$= 3 \times 3 - 8$

$= 3 \times (19 - 2 \times 8) - 8$

$= 3 \times 19 - 7 \times 8$

Continue Monday