1. Number field and field extension

§ Motivation — facterization of polynomials

x^2-2 cannot be further factorized on the rational number field, but can be factorized as $(x-\sqrt{2})(x+\sqrt{2})$ in the real number field. x^2+1 cannot be facterized in the complex numbe field but can be factorized as $(x-i)(x+i)$ in the complex number field. Rational (Q), real (R), and complex (C) are typical number fields. Q is closed under $+ - \times \div$ operations, R is closed under $\sqrt[n]{x}$ $(x \geq 0)$, and C is closed under any radical operations.

definition:

$$\boxed{\begin{array}{l}\text{A set of numbers denoted as } F\text{: ① } F \text{ contains } 0 \text{ and } 1. \\ \text{② } F \text{ is closed under } + - \times \div \text{ (divisor} \neq 0). \\ \text{Then } F \text{ is called a number field.}\end{array}}$$

Examples: ① F must contains all integers. And rational numbers Q is the minimal number field.

② Real number R and complex number C are also number fields.

But the jump from Q to R is too big. In comparison, from R to C is only to add "i" which is not that big. But Q is countable, and R is continous. We can imagine R has much more degrees of freedom that Q. We can gradually add new elements to Q to extend it. This is an example of "field extention".

Example: In order to solve $x^2-2=0$, we add $\sqrt{2}$ to Q, then we have the set of $a+b\sqrt{2}$ $(a, b \in Q)$. This also forms a number field $Q(\sqrt{2})$.

Test: $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

$$\frac{a_1+b_1\sqrt{2}}{a_2+b_2\sqrt{2}} = \frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2} + \frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}\sqrt{2}.$$

$Q(\sqrt{2})$ is the minimal number field containing Q and $\sqrt{2}$.

The set of $a+bi$ $(a, b \in Q)$ form a number field $Q(i)$, which is the minimal number field ~~on~~ containing Q and i.

When we talk about polynomials, we need to consider the set that its coefficients belong to. If the coeffients of a polynomial are defined in the field K, then it's called the polynomial on the field K. If $f(x)$ can be factorized in K, then $f(x)$ is reducible in K. For example, x^2-2 is reducible on R, but irreducible on Q, and it also reducible in $Q(\sqrt{2})$.

§ Field extension

For two number fields F and K, if $F \subset K$, then K is the extened field of F, and F is called the subfield of F.

Algebraic extension: if C is a root of an irreducible equation on F

$h_0 + h_1 x + \cdots h_n x^n = 0$, then all the numbers in the form of

$a_0 + a_1 C + \cdots a_{n-1} C^{n-1}$ with $(a_0, a_1, \cdots a_{n-1} \in F)$ form a field $F(C)$.

$F(C)$ is the algebraic extension of F, and is the minimal extension containing C. We can view $1, C, \cdots C^{n-1}$ as independent bases, and n is the relative dimension of $F(c)$ to F, denoted as

$[F(c) : F] = n$, then we say $F(c)$ is F's n-th order extension.

We can add generators c_1 and c_2 one by one. There's the following theorem:

If c_1 is a root of an irreducible equation in the field F, and c_2 is a root of an irreducible equation in the extend field $F(c_1)$, we extend $F(c_1)$ by adding c_2 and arrive at $F(c_1, c_2)$. We can also reverse the process, and arrive at $F(c_2, c_1)$, then $F(c_1 c_2) = F(c_2, c_1)$. There exis a root c of an irreducible equation on F, such that $F(c) = F(c_1, c_2) = F(c_2, c_1)$.

Example: Add $\sqrt{2}$ into $Q \rightarrow Q(\sqrt{2})$. Further add i to $Q(\sqrt{2})$, we have $Q(\sqrt{2}, i)$, which is the same as $Q(i, \sqrt{2})$. Then we can also add $c = \sqrt{2} + i$ to Q, $\longrightarrow Q(\sqrt{2} + i)$. $c = \sqrt{2} + i$ is a root of $x^4 \pm 2x^2 + 9 =$
We can show that $Q(\sqrt{2} + i) = Q(\sqrt{2}, i)$.

We can generalize it to adding $c_1, \cdots c_k$, such that the extended field $F(c_1, c_2, \cdots c_k)$ is independent on the order of adding. And there exists a "c", which is a root of an irreducible equation in F, such that

$$\boxed{F(c) = F(c_1, c_2, \cdots c_k).}$$

§ Root field and normal extension

★ $f(x)$ is a polynomial on the field F. The minimal extention K such that $f(x)$ can be completely factorized as $f(x) = (x-u_1)\cdots(x-u_n)$, in K, is called the root field. $K = F(u_1, \cdots u_n)$, and there exists a "c" — a root of an irredicible equation in F, such that $F(c) = F(u_1, \cdots u_n)$.

example: $x^3 - 2 = 0$ is an equation on Q, which has roots $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ with $\omega = e^{i\frac{2}{3}\pi}$. Its root field $Q(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = Q(\sqrt[3]{2}, \omega)$.

Obviously $[Q(\sqrt[3]{2}) ; Q] = 3$, and ω satisfies quadratic equation $x^2 + x + 1 = 0$ defined on $Q(\sqrt[3]{2})$, then $[Q(\sqrt[3]{2}, \omega) : Q(\sqrt[3]{2})] = 2$.

x^3 and higher order can be expressed as linear combinations of x and 1

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

★ Conjugate numbers:

If u and v satisfy a same irreducible equation on F, then we can u and v are conjugate on F.

example: ① $1 \pm i$ are complex conjugate since they satisfy $x^2 - 2x + 2 = 0$.

② $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ are conjugate on Q, since they satisfy $x^3 = 2$.

Case ② shows that we can have more than ~~on~~ two numbers in a conjugate set. For the field extension, it's possible that only part of the conjugate members are included: For example, $Q(\sqrt[3]{2})$ does not contain $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$.

* Normal extension

It will be much more convenient if we include all the numbers in the same conjugacy set when extending the field. This kind of extension is called the normal extension. More formally, if N is an normal extentison of F, it satisfies: For any $u \in N$, then all numbers conjugate on the field F also belong to N. There's the follwing theorem

Theorem: N is F's normal extension $\Longleftrightarrow$ N is the root field of an equation ~~ee~~ in the field of F. (Proof is complicated and omitted).

For example, for $x^3-2=0$. Its root field $Q(\sqrt[3]{2}, \omega)$ is a normal extension of Q. It contains $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$.