Q(D) is a field

Wednesday, August 9, 2017 2:10 PM

<u>Unity</u>. $[(1,1)]\cdot[(a,b)] = [(1\cdot a, 1\cdot b)] = [(a,b)]$. ■

<u>Theorem.</u> ⓐ $Q(D)$ is a field.

ⓑ $i: D \to Q(D)$, $i(a) = [(a,1)]$ is an injective ring homomorphism.

ⓒ If F is a field and $g: D \to F$ is an injective ring homomorphism, then there is an injective ring homomorphism

$$\tilde{g}: Q(D) \to F$$

such that $\tilde{g}(i(a)) = g(a)$ for any $a \in D$; and such $\tilde{g}$ is unique.

$$\begin{tikzcd}
 & D \arrow[dl, "i"'] \arrow[dr, "g"] \arrow[d, phantom, "\circlearrowleft"] & \\
Q(D) \arrow[rr, dashed, "\tilde{g}"'] & & F
\end{tikzcd}$$

<u>Pf.</u> ⓐ We have already proved that $Q(D)$ is a unital comm. ring. So it is enough to show any non-zero element in $Q(D)$ is invertible.

$$[(a,b)] \neq [(0,1)] \Rightarrow a\cdot 1 \neq b\cdot 0 \Rightarrow a \neq 0$$

$$\Rightarrow [(b,a)] \in Q(D)$$

$$[(a,b)]\cdot[(b,a)] = [(ab,ba)] \underset{\{ab\cdot 1 = ba\cdot 1\}}{=} [(1,1)] = 1_{Q(D)}$$

Main properties of Q(D)

Wednesday, August 9, 2017 2:20 PM

(b) $i(a+b) \overset{?}{=} i(a)+i(b) \iff [(a+b,1)] \overset{?}{=} \underbrace{[(a,1)]+[(b,1)]}_{[(\underbrace{a\cdot 1+1\cdot b}_{a+b},\ \underbrace{1\times 1}_{1})]}$ ✓

$i(a\cdot b) \overset{?}{=} i(a)\cdot i(b) \iff [(ab,1)] = [(a,1)]\cdot[(b,1)]$ ✓

$$\begin{aligned} a\in\ker i \iff & i(a) = [(0,1)] \\ \iff & [(a,1)] = [(0,1)] \\ \iff & a\times 1 = 1\times 0 \iff a=0. \end{aligned}$$

So i is injective.

(c) Since $g: D\to F$ is injective, $\forall a\in D\setminus\{0\}$, $g(a)\neq 0$.

So $g(a)^{-1}$ exists in F (as F is a field.)

Let $\tilde{g}: Q(D)\to F$, $\tilde{g}([(a,b)]) = g(a)\,g(b)^{-1}$.

(Notice that, since $b\neq 0$, by the above argument $g(b)^{-1}$ exists.)

<u>Claim</u>. $\tilde{g}$ is well-defined.

<u>Pf</u>. We have to show $[(a_1,b_1)] = [(a_2,b_2)]$ implies $g(a_1)g(b_1)^{-1} = g(a_2)g(b_2)^{-1}$.

$$\begin{aligned} [(a_1,b_1)] = [(a_2,b_2)] \Rightarrow a_1b_2 = a_2b_1 \Rightarrow & g(a_1)g(b_2) = g(a_2)g(b_1) \\ \Rightarrow & g(a_1)g(b_1)^{-1} = g(a_2)g(b_2)^{-1}. \end{aligned}$$

Main properties of Q(D)

Wednesday, August 9, 2017 2:29 PM

Claim. $\tilde{g}$ is a ring homomorphism.

Pf. $\tilde{g}([(a_1,b_1)]+[(a_2,b_2)]) = \tilde{g}([(a_1b_2+b_1a_2,\ b_1b_2)])$

$= g(a_1b_2+b_1a_2)\,g(b_1b_2)^{-1} = (g(a_1)g(b_2)+g(b_1)g(a_2))\,g(b_2)^{-1}g(b_1)^{-1}$

$= g(a_1)g(b_1)^{-1} + g(a_2)g(b_2)^{-1}$

$= \tilde{g}([(a_1,b_1)]) + \tilde{g}([(a_2,b_2)])$.

$\tilde{g}([(a_1,b_1)]\cdot[(a_2,b_2)]) = \tilde{g}([(a_1a_2,\ b_1b_2)])$

$= g(a_1a_2)\,g(b_1b_2)^{-1}$

$= g(a_1)\,g(a_2)\,g(b_2)^{-1}\,g(b_1)^{-1}$

$= (g(a_1)g(b_1)^{-1})(g(a_2)g(b_2)^{-1})$

$= \tilde{g}([(a_1,b_1)])\,\tilde{g}([(a_2,b_2)])$.

Claim. $\tilde{g}$ is injective

Pf. $\tilde{g}([(a,b)])=0 \Rightarrow g(a)\,g(b)^{-1}=0$

$\Rightarrow g(a)=0$

$\Rightarrow a=0$ as g is injective

$\Rightarrow [(a,b)]=[(0,b)]=[(0,1)]$.

Claim. $\tilde{g}(i(a))=g(a)$.

Pf. $\tilde{g}(i(a)) = \tilde{g}([(a,1)]) = g(a)\,g(1)^{-1}$. So it is enough to show $g(1)=1$. Notice that $g(1)^2=g(1\cdot 1)=g(1)$.

Main properties of Q(D)

Wednesday, August 9, 2017 2:42 PM

So $g(1)^2 = g(1)$. Since $1 \neq 0$, $g(1) \neq 0$. So $g(1)^{-1}$ exists.

So $g(1) = 1$.

<u>Claim</u>. There is a unique ring homomorphism $\tilde{g}: Q(D) \to F$ such that $\tilde{g}(i(a)) = g(a)$ for any $a \in D$.

<u>Pf</u>. Suppose $h: Q(D) \to F$ is a such homomorphism.

Then

$$\begin{array}{ccccc} h([(1,a)]\,[(a,1)]) & = & h([(a,a)]) = & h([(1,1)]) \\ \| & & & \| \\ h([(1,a)])\ h(i(a)) & & & h(i(1)) \\ \| & & & \| \\ h([(1,a)])\ g(a) & & & g(1) = 1 \end{array}$$

$$\Rightarrow h([(1,a)]) = g(a)^{-1}.$$

Hence

$$\begin{aligned} h([(a,b)]) &= h([(a,1)]\,[(1,b)]) \\ &= h([(a,1)])\ h([(1,b)]) \\ &= g(a)\, g(b)^{-1} = \tilde{g}([(a,b)]), \end{aligned}$$

which shows that $h = \tilde{g}$. ∎

So informally $Q(D)$ is "the smallest field" which contains a "copy of D".

Examples

Wednesday, August 9, 2017 2:52 PM

<u>Ex.</u> $Q(\mathbb{Z}) \simeq \mathbb{Q}$.

<u>Pf.</u> Since $\mathbb{Z} \xhookrightarrow{g} \mathbb{Q}$, $x \mapsto x$, by Theorem $\exists\, \tilde{g} : Q(\mathbb{Z}) \to \mathbb{Q}$,

$\tilde{g}([(a,b)]) = g(a)g(b)^{-1} = \frac{a}{b}$, and $\tilde{g}$ is injective.

Clearly $\tilde{g}$ is surjective. So $\tilde{g}$ is an isomorphism.

<u>Ex.</u> If F is a field, then $Q(F) \simeq F$.

<u>Pf.</u> Let $g : F \to F$, $g(x) = x$. By Theorem $\exists$ an injective ring homomorphism $\tilde{g} : Q(F) \to F$ such that

$\tilde{g}([(a,1)]) = g(a) = a$. So $\tilde{g}$ is surjective as well.

Hence $\tilde{g} : Q(F) \to F$ is an isomorphism.

<u>Ex.</u> Prove that $Q(\mathbb{Z}[\sqrt{2}]) \simeq \mathbb{Q}[\sqrt{2}]$ where

$\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbb{Z}\}$ and

$\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbb{Q}\}$.

<u>Pf.</u> <u>Claim 1</u>. $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$; that means

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a ring where $+, \cdot$ are the operations

in $\mathbb{R}$.

<u>Pf of claim 1</u>. For $a + \sqrt{2}\, b,\ c + \sqrt{2}\, d \in \mathbb{Q}[\sqrt{2}]$,

Q[sqrt(2)] is a field

Wednesday, August 16, 2017 1:17 AM

$$(a+\sqrt{2}b)-(c+\sqrt{2}d) = \underbrace{(a-c)}_{\text{Since in } \mathbb{Q}} + \sqrt{2}\underbrace{(b-d)}_{\text{and in } \mathbb{Q}} \in \mathbb{Q}[\sqrt{2}]$$

So $(\mathbb{Q}[\sqrt{2}],+)$ is a subgroup of $(\mathbb{R},+)$.

$$(a+\sqrt{2}b)(c+\sqrt{2}d) = \underbrace{(ac+2bd)}_{\text{Since in } \mathbb{Q}} + \sqrt{2}\underbrace{(ad+bc)}_{\text{and in } \mathbb{Q}} \in \mathbb{Q}[\sqrt{2}]$$

So $\mathbb{Q}[\sqrt{2}]$ is closed under multiplication. Hence $(\mathbb{Q}[\sqrt{2}],+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$. (Notice that we do not need to check the associativity of $\cdot$ and the distribution law as they can be deduced from the fact that $(\mathbb{R},+,\cdot)$ is a ring.)

<u>Claim 2.</u> $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$.

<u>Pf of claim 2.</u> By claim 1, we get that $\mathbb{Q}[\sqrt{2}]$ is a unital commutative ring. So it is enough to show $U(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}]\setminus\{0\}$.

Warning: we have to show $a-\sqrt{2}b \neq 0$

$$a+\sqrt{2}b \neq 0 \Rightarrow \frac{1}{a+\sqrt{2}b} = \frac{a-\sqrt{2}b}{(a+\sqrt{2}b)(a-\sqrt{2}b)} = \frac{a-\sqrt{2}b}{a^2-2b^2}$$

$$= \underbrace{\left(\frac{a}{a^2-2b^2}\right)}_{\text{in } \mathbb{Q}} - \sqrt{2}\underbrace{\left(\frac{b}{a^2-2b^2}\right)}_{\text{in } \mathbb{Q}} \in \mathbb{Q}[\sqrt{2}].$$

Sqrt(2) is irrational

Wednesday, August 16, 2017 1:30 AM

So as soon as we show: $\left.\begin{matrix} a+\sqrt{2}\,b \neq 0 \\ a,b\in\mathbb{Q} \end{matrix}\right\} \Rightarrow a-\sqrt{2}\,b \neq 0$, ⊛

we get the 2nd claim.

First we deduce ⊛ from irrationality of $\sqrt{2}$, and then we recall two proofs of irrationality of $\sqrt{2}$.

Suppose to the contrary that ⊛ does not hold. So $\exists\, a,b\in\mathbb{Q}$ s.t. $a+\sqrt{2}\,b\neq 0$ and $a-\sqrt{2}\,b=0$.

If $b\neq 0$, then $\sqrt{2}=a/b\in\mathbb{Q}$ which is a contradiction. So $b=0$. Hence $a=(\sqrt{2})(0)=0$; this implies $a+\sqrt{2}\,b=0$, which is a contradiction.

- $\sqrt{2}$ is irrational.

<u>Pf</u> (Method 1: using the unique factorization into a product of primes) Suppose to the contrary that $\sqrt{2}=\frac{m}{n}$ for $m,n\in\mathbb{Z}^+$. Then $2n^2=m^2$. Suppose $n=2^k n'$ and $m=2^\ell m'$ where $k,\ell\in\mathbb{Z}^{\geq 0}$ and m',n' are odd.

$\Rightarrow 2n^2 = 2^{2k+1}\underbrace{n'^2}_{\text{odd}} = 2^{2\ell}\underbrace{m'^2}_{\text{odd}}$. By the uniqueness of factor.

Sqrt(2) is irrational

Wednesday, August 16, 2017 1:39 AM

into primes, the power of 2 on both sides should be the same.

So $2k+1 = 2l$, which is not possible as the left hand side is odd and the right hand side is even.

(Method 2. Only using the Well-ordering principle.)

Suppose to the contrary that there are positive integers m and n such that $\sqrt{2} = \frac{m}{n}$. And so $2n^2 = m^2$. By the well-ordering principle, there is such a pair with smallest possible value of $m+n$.

Since $2 \mid m^2$, m is even. So $m = 2r$ for some $r \in \mathbb{Z}^+$. Hence $n^2 = 2r^2$. Notice that $r+n < n+m$ and $2r^2 = n^2$ which contradicts our assumption that $n+m$ is the minimum of $\{x+y \mid x, y \in \mathbb{Z}^+, \ 2x^2 = y^2\}$.

Claim 3. $Q(\mathbb{Z}[\sqrt{2}]) \simeq \mathbb{Q}[\sqrt{2}]$.

Pf. Let $g: \mathbb{Z}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$, $g(a+b\sqrt{2}) = a+b\sqrt{2}$.

Since g is an embedding and $\mathbb{Q}[\sqrt{2}]$ is a field,

Field of fractions of Z[sqrt(2)]

Wednesday, August 16, 2017 1:53 AM

the function $\tilde{g}: Q(\mathbb{Z}[\sqrt{2}]) \to \mathbb{Q}[\sqrt{2}]$,

$$\tilde{g}([(a+b\sqrt{2}, c+d\sqrt{2})]) = g(a+b\sqrt{2})\, g(c+d\sqrt{2})^{-1} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}$$

is an injective ring homomorphism. So to get an isomorphism it is enough to show $\tilde{g}$ is surjective.

$\forall\ x+\sqrt{2}\,y \in \mathbb{Q}[\sqrt{2}]$, after taking a common denominator c of x and y, we can find $a, b \in \mathbb{Z}$ s.t. $x = \frac{a}{c}$ and $y = \frac{b}{c}$. Thus $x+\sqrt{2}\,y = \frac{a}{c} + \sqrt{2}\,\frac{b}{c} = \frac{a+\sqrt{2}\,b}{c}$.

$$= g(a+\sqrt{2}b)\, g(c)^{-1}$$

$$= \tilde{g}([(a+\sqrt{2}b, c)]). \qquad \blacksquare$$

Ring of polynomials

Wednesday, August 16, 2017 1:59 AM

You have seen and worked with real or complex polynomials in a given variable x. We can and will consider polynomials with coefficients in a given ring in an indeterminant x:

$$R[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n \mid n\in\mathbb{Z}^{\geq 0},\ a_i\in R\}.$$

We sometimes write $\sum_{i=0}^{n} a_i x^i$ instead of $a_0+a_1x+\cdots+a_nx^n$.

Or $\sum_{i=0}^{\infty} a_i x^i$ with an understanding that $a_{n+1}=a_{n+2}=\cdots=0$ for some $n\in\mathbb{Z}^{\geq 0}$.

$R[x]$ with the usuall $+$ and $\cdot$ is a ring. Here is the formal definition:

$$\sum_{i=0}^{\infty} a_i x^i+\sum_{i=0}^{\infty} b_i x^i=\sum_{i=0}^{\infty}(a_i+b_i)x^i, \text{ and}$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right)=\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right)x^n.$$

Ex. Find $(x+1)^5$ in $\mathbb{Z}_4[x]$.

Solution $(x+1)^2=x^2+2x+1$.

$$\begin{aligned}(x+1)^4=(x^2+2x+1)^2&=x^4+2x^3+x^2\\&\quad+2x^3+0+2x\\&\quad+x^2+2x+1\\&=x^4+2x^2+1 \Rightarrow (x+1)^5=x^5+x^4+2x^3+2x^2+x+1.\end{aligned}$$