Série 9

David Wiedemann

2 mai 2022

1

First, notice that ϕ will fix $\mathbb{Z}$, indeed, since $\phi(1) = 1$ and $\phi(-1)+\phi(1) = 0 \implies \phi(-1) = -1$, we have that $\forall a \in \mathbb{Z}$, if a is positive

$$\phi(a) = \phi(1 + 1 \ldots + 1) = 1 + \ldots + 1 = a$$

and if a is negative

$$\phi(a) = \phi(-1 - \ldots - 1) = -1 - \ldots - 1 = a$$

Now, pick an element $\frac{p}{q}$ of $\mathbb{Q}$, then $q \cdot \frac{p}{q} = p$ and thus

$$p = \phi(p) = \phi\left(q \cdot \frac{p}{q}\right) = \phi(q) \cdot \phi\left(\frac{p}{q}\right) = q \cdot \phi\left(\frac{p}{q}\right)$$

Hence $\phi(\frac{p}{q}) = \frac{p}{q}$ which shows that ϕ restricted to $\mathbb{Q}$ is the identity.

2

Let us denote $S \coloneqq \{s \in F | \exists a, b \in \mathbb{Z} : s^2 + as + b = 0\}$.
We show the double inclusion.

$A \subset S$

Let $x + y\sqrt{-d} \in A$ (ie. $x, y \in \mathbb{Z}$).
Let $a = -2x$ and $b = y^2d + x^2$, then note that

$$\begin{aligned}
&(x + y\sqrt{-d})^2 + a(x + y\sqrt{-d}) + b \\
&= x^2 + 2xy\sqrt{-d} - y^2d + ax + ay\sqrt{-d} + b \\
&= (x^2 - y^2d^2 + ax + b) + (2xy + ay)\sqrt{-d} \\
&= (x^2 - y^2d^2 - 2x^2 + y^2d + x^2) + (2xy - 2xy)\sqrt{-d} = 0
\end{aligned}$$

Which show the inclusion $A \subset S$

$A \supset S$

Given $s \in F$, since F is a quadratic (finite) extension of $\mathbb{Q}$ and thus $\mathbb{Q}\left(\sqrt{-d}\right) = \mathbb{Q}\left[\sqrt{-d}\right]$, we may write s as $s = \frac{p}{q} + \frac{x}{y}\sqrt{-d}$, where we suppose $p, q, x, y \in \mathbb{Z}$ and $(p, q) = (x, y) = 1$.
Let us now first suppose that $\frac{p}{q}, \frac{x}{y} \neq 0$, we'll treat these special cases later.
Let $a, b \in \mathbb{Z}$ such that $s^2 + as + b = 0$.
Plugging $s = \frac{p}{q} + \frac{x}{y}\sqrt{-d}$ into the polynomial yields

$$\frac{p^2}{q^2} - 2\frac{p}{q}\frac{x}{y}\sqrt{-d} - \frac{x^2}{y^2}d + a\frac{p}{q} + a\frac{x}{y}\sqrt{-d} + b = 0$$

as $\sqrt{-d}$ and 1 are linearly independent over $\mathbb{Q}$, we get the system of equations

$$\frac{p^2}{q^2} - \frac{x^2}{y^2}d + a\frac{p}{q} + b = 0 \tag{1}$$

$$-2\frac{p}{q}\frac{x}{y} + a\frac{p}{q} = 0 \tag{2}$$

From equation 2 above we deduce (and by our assumption that $\frac{p}{q} \neq 0$) that

$$-2\frac{x}{y} + a = 0$$

By coprimality of x and y, this implies that $y = 1$ or $y = 2$, we treat these cases separately :

If $y = 1$

So suppose $\frac{p}{q} \in \mathbb{Q} \setminus \mathbb{Z}$, ie. $q \neq 1$.
Rewriting equation 1 above then yields

$$\begin{aligned} \frac{p^2}{q^2} - x^2d + a\frac{p}{q} + b &= 0 \\ p^2 - x^2dq^2 + apq + bq^2 &= 0 \\ x^2dq^2 &= p^2 + apq + bq^2 \end{aligned}$$

Since $q|x^2dq^2$, $q|p^2 + apq + bq^2 \implies q|p^2$ which is a contradicition, since we supposed that p and q share no common factors and $q \neq 1$.
Thus $q = 1$ and $s = p + x\sqrt{-d}$.

If $y = 2$

By equation 2 above, we know that then $x = a$. This implies in particular that a is not a multiple of 2 as $(x, 2) = 1$. Plugging this into equation 1

yields :

$$\frac{p^2}{q^2} - \frac{a^2}{4}d + a\frac{p}{q} + b = 0$$
$$4p^2 - a^2dq^2 + 4apq + 4bq^2 = 0$$
$$a^2dq^2 = 4p^2 + 4apq + 4bq^2$$

Now, since d is square free and a is not a multiple of 2, $4|q^2$ and in particular $2|q$, thus rewrite $q = 2e$ for some integer $e \in \mathbb{Z}$.

$$a^2d4e^2 = 4p^2 + 4ap2e + 4b4e^2$$
$$a^2de^2 = p^2 + 2ape + 4be^2$$

Reducing the above modulo 4 yields the congruence relation

$$a^2de^2 \equiv p^2 + 2ape \mod 4 \tag{3}$$

Now, if e is a multiple of 2, then the above relation simply reduces to

$$0 \equiv p^2 \mod 4$$

Which implies $4|p^2 \implies 2|p$ which would mean $\frac{p}{q}$ is not irreducible, a contradiction.
Thus, suppose e is not a multiple of 2.
It now suffices to check that this is impossible for the different congruence classes of d modulo 4.

If $d \equiv 0 \mod 4$

Then d is divisible by 4, but d is square free, which is impossible.

If $d \equiv 1 \mod 4$

Notice that an uneven number squared is always congruent to 1 modulo 4, since $(2k+1)^2 \equiv 4k^2 + 4k + 1 \equiv 1 \mod 4$.
Using this, in equation 3 above yields with $d \equiv 1 \mod 4$.

$$a^2e^2 \equiv p^2 + 2ape \mod 4$$
$$1 \cdot 1 \equiv 1 + 2(1 \cdot 1 \cdot 1) \mod 4$$

Where we used that a, e and p are all uneven and that reduction modulo some integer is a morphism of rings.
But $1 \not\equiv 3 \mod 4$ and we get a contradiction.

If $d \equiv 2 \mod 4$

Further reducing the congruence relation in 3 yields

$$0 \equiv p^2 \mod 2$$

Whence $2|p^2 \implies 2|p$ which is a contradiction.

Hence, we have eliminated all possibilities for the values of d.
It remains to show the special cases mentionned at the start.

If $\frac{x}{y} = 0$

We may suppose $\frac{p}{q} \neq 0$ and that $(p, q) = 1$ then plugging this into our quadratic equation yields

$$\begin{aligned} \frac{p^2}{q^2} + a\frac{p}{q} + b &= 0 \\ p^2 + apq + bq^2 &= 0 \\ p^2 &= -q(ap + bq) \end{aligned}$$

But then $q|p^2$ and thus $q = 1$ by our hypothesis

If $\frac{p}{q} = 0$

Again, recall $(p, q) = 1$ Then plugging $\frac{p}{q}\sqrt{-d}$ into the equation yields

$$-d\frac{p^2}{q^2} + a\frac{p}{q}\sqrt{-d} + b = 0$$

Now, if $a \neq 0$ this equation can not hold since $\sqrt{-d}$ and 1 are linearly independent over $\mathbb{Q}$.
If $a = 0$, then rewriting the above gives

$$dp^2 = bq^2$$

Whence, since $(p, q) = 1$ $q^2|d$ which contradicts our hypothesis.

And that's it for part 2 (whew).

3

First, notice that we may apply the results from section 2 to $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-5})$ as both 1 and 5 are square free and congruent to 1 $\mod 4$.
Suppose $\phi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{-5})$ is an isomorphism.
Notice that then ϕ induces an isomorphism of rings between $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$.

Indeed, let $s \in \mathbb{Q}(i)$ be integral over $\mathbb{Z}$, ie. an element such that $s^2+as+b=0$ for some integers a and b, then applying ϕ to this gives an element $\phi(s)$ satisfying

$$\phi(s)^2 + a\phi(s) + b = 0 \quad \text{(since } \phi \text{ fixes } \mathbb{Q})$$

Which will thus be integral in $\mathbb{Q}(\sqrt{-5})$ over $\mathbb{Z}$, ie. is an element of $\mathbb{Z}[\sqrt{-5}]$, it is clear that this mapping is an isomorphism with inverse ϕ^{-1} .
Now we prove that $\mathbb{Z}[i] \not\cong \mathbb{Z}[\sqrt{-5}]$ which will contradict the fact that ϕ is an isomorphism.

Indeed, let ψ be such an isomorphism, by the same argument as in 1, ψ fixes $\mathbb{Z}$.
Thus $\psi^{-1}(\sqrt{-5})^2 = -5$.
Let $a + bi = \psi^{-1}(\sqrt{-5})$ be such an element, then $a^2 + 2abi - b^2 = -5$, implying either a or b equal to 0, since $a^2 - b^2 = -5$ and $a^2, b^2 > 0$, this implies $a = 0$ and thus $-b^2 = -5$.
But 5 is prime and thus such a b cannot exist, contradicting the fact that ψ is an isomorphism.