| EPFL - Printemps 2022 | Prof. Z. Patakfalvi |
|---|---|
| **Anneaux et Corps** | **Exercices** |
| Solutions Bonus Series 9 | |

**Exercice 7.** 1. Since $\phi$ is a ring homomorphis we have $\phi(1) = 1$. Therefore $\phi$ fixes the element in $\mathbb{Z}$. To see that $\phi$ fixes also the elements in $\mathbb{Q}$ note that for every

$$\frac{p}{q} \in \mathbb{Q}$$

where $p, q \in \mathbb{Z}$ and $q \neq 0$ we have that

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

therefore

$$\phi(\frac{p}{q}) = \frac{p}{q}.$$

2. Set $T = \{s \in F | \exists a, b \in \mathbb{Z} : s^2 + as + b = 0\}$. Take $s \in T$. We know that $s = r + ti\sqrt{d}$ for $r$ and $t \in \mathbb{Q}$. Then, we have

$$(r + ti\sqrt{d})^2 - 2r(r + ti\sqrt{d}) + (r^2 + t^2 d) = 0$$

So, the minimal polynomial of $s$ over $\mathbb{Q}$ is

$$m = x^2 - 2rx + (r^2 + t^2 d)$$

In particular, all polynomials of degree 2, which have s as roots, are multiples of m by a rational number. So, the only way $s$ can satisfy a polynomial with integer coefficients and 1 as the leading coefficient is if $2r \in \mathbb{Z}$ and $r^2 + t^2 d \in \mathbb{Z}$. From the first condition we may write $r = r'/2$ for $r' \in \mathbb{Z}$. Then we have

$$r^2 + t^2 d = r'^2/4 + t^2 d \in \mathbb{Z}$$

We obtain that $4t^2 d \in \mathbb{Z}$, so using that $d$ is square-free we may write t also as $t'/2$ for $t \in \mathbb{Z}$. Then we have

$$(r'^2 + t'^2 d)/4 \in \mathbb{Z}$$

Equivalently we have

$$4 | r'^2 + t'^2 d$$

Taking into account that $d \equiv 1 \mod 4$ and that square numbers are 0 or $1 mod 4$ we obtain that the only solution is that both $r'$ and $t'$ is divisible by 2. This implies that $r$ and $t$ are actually integers. This concludes the proof that $T \subseteq A$.

For the other inclusion if $s \in A$, then the formula $m = x^2 - 2rx + (r^2 + t^2 d)$ shows that in fact $s \in T$.

3. Set $d = 1$ and $d = 5$, define $T' = \{s \in F' | \exists a, b \in \mathbb{Z} : s^2 + as + b = 0\}$, and let $\phi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{-5})$ be an isomorphism.

   The previous two points gives that $\phi$ induces a (ring) isomorphism $A \to A'$. In particular, from point 2) we have that $A = T$ and $A' = T'$ and $\phi$ fixes $\mathbb{Z}$, so $\phi$ sends every element satisfying a degree 2 polynomial with coefficients over $\mathbb{Z}$ and leading coefficient 1 to an element with the same properties.

   However $A \ncong A'$, as we have seen earlier in the course that $A$ is a UFD, but $A'$ is not. Therefore $\mathbb{Q}(i)$ cannot be isomorphic to $\mathbb{Q}(\sqrt{-5})$