ALGEBRAIC NUMBER THEORY

HOMEWORK 1

(1) Show that $6 = (1+\sqrt{-5}\,)(1-\sqrt{-5}\,) = 2\cdot 3$ is another example of nonunique factorization in $\mathbb{Z}[\sqrt{-5}\,]$.

We claim that $1+\sqrt{-5}$ is irreducible. In fact, assume that $1+\sqrt{-5} = \alpha\beta$; taking norms gives $6 = N\alpha N\beta$. Since there are no elements of norm 2 or 3 in $\mathbb{Z}[\sqrt{-5}\,]$, we must have $N\alpha = 1$ or $N\beta = 1$, which implies $\alpha = \pm 1$ or $\beta = \pm 1$. This proves our claim.

Since $1+\sqrt{-5}$ is irreducible, so is $1-\sqrt{-5}$: in fact, conjugating $1-\sqrt{-5} = \alpha\beta$ gives $1+\sqrt{-5} = \alpha'\beta'$. By what we have proved, $\alpha' = \pm 1$ or $\beta' = \pm 1$, and taking conjugates once more we get $\alpha = \pm 1$ or $\beta = \pm 1$.

Similar arguments work for 2 and 3.

(2) Explain the different factorizations in Problem 1 using the ideals $\mathfrak{p} = (2, 1+\sqrt{-5}\,)$, $\mathfrak{q} = (3, 1-\sqrt{-5}\,)$, and $\mathfrak{q}' = (3, 1+\sqrt{-5}\,)$. Show that
(a) $(2, 1-\sqrt{-5}\,) = \mathfrak{p}$;
(b) $\mathfrak{p}^2 = (2)$;
(c) $\mathfrak{q}\mathfrak{q}' = (3)$;
(d) $\mathfrak{q}^2 = (2+\sqrt{-5}\,)$.

(a) $(2, 1-\sqrt{-5}\,) = \mathfrak{p}$: this is clear since $1+\sqrt{-5} = 1-\sqrt{-5}+\sqrt{-5}\cdot 2$ and $1-\sqrt{-5} = 1+\sqrt{-5}-\sqrt{-5}\cdot 2$.

(b) $\mathfrak{p}^2 = (2)$:

$$\begin{aligned}\mathfrak{p}^2 = \mathfrak{p}\mathfrak{p}' &= (2, 1+\sqrt{-5}\,)(2, 1-\sqrt{-5}\,)\\ &= (4, 2(1+\sqrt{-5}\,), 2(1-\sqrt{-5}\,), 6)\\ &= (2)(2, 1+\sqrt{-5}, 1-\sqrt{-5}, 3) = (2)\end{aligned}$$

because any ideal containing 2 and 3 contains $1 = 3-2$ and therefore is the unit ideal.

(c) $\mathfrak{q}\mathfrak{q}' = (3)$:

$$\begin{aligned}\mathfrak{q}\mathfrak{q}' &= (3, 1+\sqrt{-5}\,)(3, 1-\sqrt{-5}\,)\\ &= (9, 3(1+\sqrt{-5}\,), 3(1-\sqrt{-5}\,), 6)\\ &= (3)(3, 1+\sqrt{-5}, 1-\sqrt{-5}, 2) = (3).\end{aligned}$$

(d) $\mathfrak{q}^2 = (2+\sqrt{-5}\,)$:

$$\begin{aligned}\mathfrak{q}^2 &= (9, 3(1-\sqrt{-5}, -4-2\sqrt{-5}\,)\\ &= (2+\sqrt{-5}\,)(2-\sqrt{-5}, 1+\sqrt{-5}, 2) = (2+\sqrt{-5}\,)\end{aligned}$$

since the second factor contains 2 and $2-\sqrt{-5}$, hence 2 and $(2-\sqrt{-5}\,)(2+\sqrt{-5}\,) = 9$, and thus $1 = 9-4\cdot 2$.

(3) Show that $6 = 2 \cdot 3 = (2+\sqrt{-2}\,)(2-\sqrt{-2}\,)$ is not an example of nonunique factorization in $\mathbb{Z}[\sqrt{-2}\,]$. This is not an example of nonunique factorization in $\mathbb{Z}[\sqrt{-2}\,]$ because the factors are not irreducible: we have $2 = -\sqrt{-2}^2$, $3 = (1+\sqrt{-2}\,)(1-\sqrt{-2}\,)$, $(2+\sqrt{-2}\,) = \sqrt{-2}(1-\sqrt{-2}\,)$ and $(2-\sqrt{-2}\,) = -\sqrt{-2}(1+\sqrt{-2}\,)$. In particular, the complete factorization of 6 into irreducibles is

$$6 = -\sqrt{-2}^2(1+\sqrt{-2}\,)(1-\sqrt{-2}\,);$$

the factorizations given in the problem are obtained by pairing up these irreducible factors.

(4) Compute the characteristic polynomial of $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with respect to the $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ of $\mathbb{Q}(\sqrt[3]{2})$. We find

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt[3]{2} + c\sqrt[3]{4}, \\ \alpha \cdot \sqrt[3]{2} &= 2c + a\sqrt[3]{2} + b\sqrt[3]{4}, \\ \alpha \cdot \sqrt[3]{4} &= 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}. \end{aligned}$$

Thus the characteristic polynomial of α is given by

$$\begin{aligned} P_\alpha(X) &= -\begin{vmatrix} a-X & 2c & 2b \\ b & a-X & 2c \\ c & b & a-X \end{vmatrix} \\ &= X^3 - 3aX^2 + (3a^2 - 6bc)X - (a^3 + 2b^3 + 4c^3 - 6abc). \end{aligned}$$

In particular, $N\alpha = a^3 + 2b^3 + 4c^3 - 6abc$.