Solutions 2

1. The ring of integers in K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Proof: Let $\alpha = a + b\sqrt{-5} \in K$ be an algebraic integer (where $a, b \in \mathbb{Q}$), then $\overline{\alpha} = a - b\sqrt{-5} \in \mathcal{O}_K$ too, hence $2a = \alpha + \overline{\alpha} \in \mathcal{O}_K$ and $a^2 + 5b^2 = \alpha\overline{\alpha} \in \mathcal{O}_K$. So $2a, a^2 + 5b^2 \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Then $5(2b)^2 = 4(a^2 + 5b^2) - (2a)^2 \in \mathbb{Z}$, so $2b \in \mathbb{Z}$. Using the notation $A = 2a$, $B = 2b$, we get that $4 \mid A^2 + 5B^2$, which is only possible if $2 \mid A, B$. So indeed $a, b \in \mathbb{Z}$.

a) The ideals (2), (3), (5), (7) factorize in $\mathcal{O}_K$ as follows:

$$\begin{aligned}(2) &= (2, 1 + \sqrt{-5})^2,\\ (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}),\\ (5) &= (\sqrt{-5})^2,\\ (7) &= (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}).\end{aligned}$$

The same way as we have done in Ex. 1/1, we can show that the ideals $\mathfrak{p}_1 = (2, 1 + \sqrt{-5})$, $\mathfrak{p}_2 = (3, 1 + \sqrt{-5})$, $\mathfrak{p}_3 = (3, 1 - \sqrt{-5})$, $\mathfrak{p}_4 = (\sqrt{-5})$, $\mathfrak{p}_5 = (7, 3 + \sqrt{-5})$, $\mathfrak{p}_6 = (7, 3 - \sqrt{-5})$ are maximal ideals of $\mathcal{O}_K$, with residue fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_7$. So $e_{\mathfrak{p}_1/2} = 2$, $e_{\mathfrak{p}_2/3} = e_{\mathfrak{p}_3/3} = 1$, $e_{\mathfrak{p}_4/5} = 2$, $e_{\mathfrak{p}_5/7} = e_{\mathfrak{p}_6/7} = 1$, and $f_{\mathfrak{p}_1/2} = f_{\mathfrak{p}_2/3} = f_{\mathfrak{p}_3/3} = f_{\mathfrak{p}_4/5} = f_{\mathfrak{p}_5/7} = f_{\mathfrak{p}_6/7} = 1$. So

$$\begin{aligned}[K : \mathbb{Q}] = 2 = e_{\mathfrak{p}_1/2} f_{\mathfrak{p}_1/2} = e_{\mathfrak{p}_2/3} f_{\mathfrak{p}_2/3} + e_{\mathfrak{p}_3/3} f_{\mathfrak{p}_2/3} = e_{\mathfrak{p}_4/5} f_{\mathfrak{p}_4/5} =\\ = e_{\mathfrak{p}_5/7} f_{\mathfrak{p}_5/7} + e_{\mathfrak{p}_6/7} f_{\mathfrak{p}_6/7}.\end{aligned}$$

b) Using $n_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$, we get that $n_{\mathfrak{p}_1} = 2$, $n_{\mathfrak{p}_2} = n_{\mathfrak{p}_3} = 1$, $n_{\mathfrak{p}_4} = 2$, $n_{\mathfrak{p}_5} = n_{\mathfrak{p}_6} = 1$. (One can also calculate $n_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$ explicitly, using the decomposition of the polynomial $X^2 + 5 \in \mathbb{Q}_p[X]$.)

The product formula says that $\prod_\nu |x|_\nu^{n_\nu} = 1$.

There are two conjugate embeddings of K into $\mathbb{C}$, so K has just one archimedean place $|\cdot|_\infty$, with $n_\infty = 2$. Moreover $|2|_\infty = 2$, $|3|_\infty = 3$, $|5|_\infty = 5$, $|7|_\infty = 7$.

The non-archimedean places of K are $|\cdot|_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through the prime ideals of $\mathcal{O}_K$. We will use the formula $|x|_{\mathfrak{p}} = p^{-v_{\mathfrak{p}}(x)/e_{\mathfrak{p}}}$. We have $v_{\mathfrak{p}_1}(2) = 2$, $v_{\mathfrak{p}_2}(3) = v_{\mathfrak{p}_3}(3) = 1$, $v_{\mathfrak{p}_4}(5) = 2$, $v_{\mathfrak{p}_5}(7) = v_{\mathfrak{p}_6}(7) = 1$, so $|2|_{\mathfrak{p}_1} = \frac{1}{2}$, $|3|_{\mathfrak{p}_2} =$

Bitte wenden!

$|3|_{\mathfrak{p}_3} = \frac{1}{3}$, $|5|_{\mathfrak{p}_4} = \frac{1}{5}$, $|7|_{\mathfrak{p}_5} = |7|_{\mathfrak{p}_6} = \frac{1}{7}$ (these are not surprising, since $|\cdot|_{\mathfrak{p}}$ extends $|\cdot|_p$, and $|p|_p = \frac{1}{p}$).

Now we can check the product formula:

$$\begin{aligned}
x = 2: &\quad |2|_\infty^{n_\infty} \cdot |2|_{\mathfrak{p}_1}^{n_1} = 4 \cdot (\tfrac{1}{2})^2 = 1,\\
x = 3: &\quad |3|_\infty^{n_\infty} \cdot |3|_{\mathfrak{p}_2}^{n_2} \cdot |3|_{\mathfrak{p}_3}^{n_3} = 9 \cdot \tfrac{1}{3} \cdot \tfrac{1}{3} = 1,\\
x = 5: &\quad |5|_\infty^{n_\infty} \cdot |5|_{\mathfrak{p}_4}^{n_4} = 25 \cdot (\tfrac{1}{5})^2 = 1,\\
x = 7: &\quad |7|_\infty^{n_\infty} \cdot |7|_{\mathfrak{p}_5}^{n_5} \cdot |7|_{\mathfrak{p}_6}^{n_6} = 49 \cdot \tfrac{1}{7} \cdot \tfrac{1}{7} = 1.
\end{aligned}$$

2. We have seen in Ex. 1/2 that the ring of integers in $K = \mathbb{Q}(\sqrt[3]{2})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. The solution of this exercise is similar to the solution of Ex. 2/1.

a) The ideals (2), (3), (5), (7) factorize in $\mathcal{O}_K$ as follows:

$$\begin{aligned}
(2) &= (\sqrt[3]{2})^3,\\
(3) &= (1+\sqrt[3]{2})^3,\\
(5) &= (1+\sqrt[3]{4})(1+2\sqrt[3]{2}-\sqrt[3]{4}),\\
(7) &= (7).
\end{aligned}$$

The same way as we have done in Ex. 1/1, we can show that the ideals $\mathfrak{p}_1 = (\sqrt[3]{2})$, $\mathfrak{p}_2 = (1+\sqrt[3]{2})$, $\mathfrak{p}_3 = (1+\sqrt[3]{4})$, $\mathfrak{p}_4 = (1+2\sqrt[3]{2}-\sqrt[3]{4})$, $\mathfrak{p}_5 = (7)$ are maximal ideals of $\mathcal{O}_K$, with residue fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_{343}$. So $e_{\mathfrak{p}_1/2} = 3$, $e_{\mathfrak{p}_2/3} = 3$, $e_{\mathfrak{p}_3/5} = e_{\mathfrak{p}_4/5} = 1$, $e_{\mathfrak{p}_5/7} = 1$, and $f_{\mathfrak{p}_1/2} = 1$, $f_{\mathfrak{p}_2/3} = 1$, $f_{\mathfrak{p}_3/5} = 1$, $f_{\mathfrak{p}_4/5} = 2$, $f_{\mathfrak{p}_5/7} = 3$. So

$$[K:\mathbb{Q}] = 3 = e_{\mathfrak{p}_1/2} f_{\mathfrak{p}_1/2} = e_{\mathfrak{p}_2/3} f_{\mathfrak{p}_2/3} = e_{\mathfrak{p}_3/5} f_{\mathfrak{p}_3/5} + e_{\mathfrak{p}_4/5} f_{\mathfrak{p}_4/5} = e_{\mathfrak{p}_5/7} f_{\mathfrak{p}_5/7}.$$

b) Using $n_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$, we get that $n_{\mathfrak{p}_1} = 3$, $n_{\mathfrak{p}_2} = 3$, $n_{\mathfrak{p}_3} = 1$, $n_{\mathfrak{p}_4} = 2$, $n_{\mathfrak{p}_5} = 3$. (One can also calculate $n_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$ explicitly, using the decomposition of the polynomial $X^3 - 2 \in \mathbb{Q}_p[X]$.)

The product formula says that $\prod_\nu |x|_\nu^{n_\nu} = 1$.

There are three embeddings of K into $\mathbb{C}$: $\sigma_1, \sigma_2, \sigma_3$, where $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}$ and $\sigma_3(\sqrt[3]{2}) = \varepsilon^2\sqrt[3]{2}$ (here $\varepsilon = e^{2\pi i/3}$). Then σ_1 is a real embedding, while σ_2 and σ_3 are conjugate complex embeddings. So K has two archimedean places, $|\cdot|_\infty$ and $|\cdot|_{\infty'}$, where $|\cdot|_\infty$ is the place corresponding to σ_1, and $|\cdot|_{\infty'}$ is the place corresponding to σ_2 and $\sigma_3 = \overline{\sigma_2}$. Clearly $n_\infty = 1$ (real embedding) and $n_{\infty'} = 2$ (non-real embedding). Moreover $|2|_\infty = |2|_{\infty'} = 2$, $|3|_\infty = |3|_{\infty'} = 3$, $|5|_\infty = |5|_{\infty'} = 5$, $|7|_\infty = |7|_{\infty'} = 7$.

The non-archimedean places of K are $|\cdot|_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through the prime ideals of $\mathcal{O}_K$. We will use the formula $|x|_{\mathfrak{p}} = p^{-v_{\mathfrak{p}}(x)/e_{\mathfrak{p}}}$. We have $v_{\mathfrak{p}_1}(2) = 3$,

Siehe nächstes Blatt!

$v_{\mathfrak{p}_2}(3) = 3$, $v_{\mathfrak{p}_3}(5) = v_{\mathfrak{p}_4}(5) = 1$, $v_{\mathfrak{p}_5}(7) = 1$, so $|2|_{\mathfrak{p}_1} = \frac{1}{2}$, $|3|_{\mathfrak{p}_2} = \frac{1}{3}$, $|5|_{\mathfrak{p}_3} = |5|_{\mathfrak{p}_4} = \frac{1}{5}$, $|7|_{\mathfrak{p}_5} = \frac{1}{7}$ (these are not surprising, since $|\cdot|_{\mathfrak{p}}$ extends $|\cdot|_p$, and $|p|_p = \frac{1}{p}$).

Now we can check the product formula:

$$\begin{aligned}
x = 2: &\quad |2|_\infty^{n_\infty} \cdot |2|_{\infty'}^{n_{\infty'}} \cdot |2|_{\mathfrak{p}_1}^{n_1} = 2 \cdot 4 \cdot (\tfrac{1}{2})^3 = 1,\\
x = 3: &\quad |3|_\infty^{n_\infty} \cdot |3|_{\infty'}^{n_{\infty'}} \cdot |3|_{\mathfrak{p}_2}^{n_2} = 3 \cdot 9 \cdot (\tfrac{1}{3})^3 = 1,\\
x = 5: &\quad |5|_\infty^{n_\infty} \cdot |5|_{\infty'}^{n_{\infty'}} \cdot |5|_{\mathfrak{p}_3}^{n_3} \cdot |5|_{\mathfrak{p}_4}^{n_4} = 5 \cdot 25 \cdot \tfrac{1}{5} \cdot (\tfrac{1}{5})^2 = 1,\\
x = 7: &\quad |7|_\infty^{n_\infty} \cdot |7|_{\infty'}^{n_{\infty'}} \cdot |7|_{\mathfrak{p}_5}^{n_5} = 7 \cdot 49 \cdot (\tfrac{1}{7})^3 = 1.
\end{aligned}$$

3. **a)** Let $\mathcal{O}$ denote the ring of algebraic integers in $\mathbb{C}$. We know that $\sigma_i(\omega_j) \in \mathcal{O}$ for every i, j. We have

$$d = \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)})$$

and

$$d' = \sum_{\pi \in \mathfrak{S}_n} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)}),$$

so

$$\frac{d' - d}{2} = \sum_{\pi \in \mathfrak{S}_n,\, \operatorname{sgn}(\pi) = 1} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)}).$$

These are all polynomials (with coefficients in $\mathbb{Z}$) of $\sigma_i(\omega_j)$, hence $d, d', \frac{d'-d}{2} \in \mathcal{O}$.

b) Let us take a (finite) Galois extension $L/\mathbb{Q}$ such that $L \subseteq \mathbb{C}$ and $\sigma_i(\omega_j) \in L$ for every i and j. We will use the basic fact from Galois theory, that if $\alpha \in L$ is fixed by all elements of the Galois group $\operatorname{Gal}(L/\mathbb{Q})$, then $\alpha \in \mathbb{Q}$. Since d' is a polynomial (with coefficients in $\mathbb{Z}$) of $\sigma_i(\omega_j)$, we have $d' \in L$. To prove that $d' \in \mathbb{Q}$, it is enough to show that $\tau(d') = d'$ for every $\tau \in \operatorname{Gal}(L/\mathbb{Q})$. This is true, because $\tau\sigma_i$ is an embedding of K into $\mathbb{C}$, hence $\tau\sigma_1, \ldots, \tau\sigma_n$ is a permutation of $\sigma_1, \ldots, \sigma_n$, so τ permutes the rows of $(\sigma_i(\omega_j))$, and the permanent is invariant under the permutation of its rows. So indeed $d' \in \mathbb{Q}$.

Using a), we get that $d' \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

c) We have

$$\begin{aligned}
\Delta_K = d^2 = (d' + (d - d'))^2 = d'^2 + 2d(d - d') + (d - d')^2 = \\
= d'^2 + 4\left(d\frac{d - d'}{2} + \left(\frac{d - d'}{2}\right)^2\right).
\end{aligned}$$

Bitte wenden!

Here $\Delta_K \in \mathbb{Z}$ and $d' \in \mathbb{Z}$, so $A := d\frac{d-d'}{2} + (\frac{d-d'}{2})^2 = \frac{1}{4}(\Delta_K - d'^2) \in \mathbb{Q}$. On the other hand $d, \frac{d-d'}{2} \in \mathcal{O}$, so $A \in \mathcal{O}$ too. Thus $A \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$, therefore $\Delta_K = d'^2 + 4A \equiv d'^2 \pmod 4$. Since $d' \in \mathbb{Z}$, this implies that $\Delta_K \equiv 0$ or $1 \pmod 4$.

4. **a)** Let $N(a+bi) := |a+bi|^2 = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$ (where $a, b \in \mathbb{Z}$), then $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $N\colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$. To prove this, let $u, v \in \mathbb{Z}[i]$, $v \neq 0$. We will show that there are elements $q, r \in \mathbb{Z}[i]$ such that $u = qv + r$ and $N(r) < N(v)$.

Note that $u = qv + r \Leftrightarrow \frac{u}{v} = q + \frac{r}{v}$. The idea is to find the nearest element of the lattice $\mathbb{Z} + \mathbb{Z}i$ to $\frac{u}{v} \in \mathbb{C}$. Let $\frac{u}{v} = \alpha + \beta i$, where $\alpha, \beta \in \mathbb{Q}$. Then there exist unique $a, b \in \mathbb{Z}$ such that $a \in [\alpha - \frac{1}{2}, \alpha + \frac{1}{2})$ and $b \in [\beta - \frac{1}{2}, \beta + \frac{1}{2})$. Let $q = a + bi \in \mathbb{Z}[i]$ and $r = u - qv \in \mathbb{Z}[i]$, then

$$\left|\frac{r}{v}\right| = \left|\frac{u}{v} - q\right| = |(\alpha - a) + (\beta - b)i| \leq \sqrt{(1/2)^2 + (1/2)^2} = \frac{1}{\sqrt{2}} < 1,$$

so $N(r) = |r|^2 < |v|^2 = N(v)$.

b) Let $N(\alpha + \beta\sqrt{2}) := |(\alpha + \beta\sqrt{2})(\alpha - \beta\sqrt{2})| = |\alpha^2 - 2\beta^2|$ for every $\alpha, \beta \in \mathbb{Q}$. Then $N\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{R}_{\geq 0}$, and $N(xy) = N(x)N(y)$ for every $x, y \in \mathbb{Q}(\sqrt{2})$. We claim that $N|_{\mathbb{Z}[\sqrt{2}]}\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_{\geq 0}$ is a Euclidean function for the ring $\mathbb{Z}[\sqrt{2}]$. To prove this, let $u, v \in \mathbb{Z}[\sqrt{2}]$, $v \neq 0$. We will show that there are elements $q, r \in \mathbb{Z}[\sqrt{2}]$ such that $u = qv + r$ and $N(r) < N(v)$.

First note that $N(v) > 0$, since $v \neq 0$. Let $\frac{u}{v} = \alpha + \beta\sqrt{2}$, where $\alpha, \beta \in \mathbb{Q}$. Then there exist unique $a, b \in \mathbb{Z}$ such that $a \in [\alpha - \frac{1}{2}, \alpha + \frac{1}{2})$ and $b \in [\beta - \frac{1}{2}, \beta + \frac{1}{2})$. Let $q = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $r = u - qv \in \mathbb{Z}[\sqrt{2}]$, then

$$\begin{aligned} N\left(\frac{r}{v}\right) = N\left(\frac{u}{v} - q\right) = N((\alpha - a) + (\beta - b)\sqrt{2}) \leq \\ \leq \max\left(|\alpha - a|^2, 2|\beta - b|^2\right) \leq \frac{1}{2} < 1, \end{aligned}$$

so $N(r) = N(\frac{r}{v})N(v) < N(v)$.

c) We have the multiplicative norm $N(a+bi) = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$ on $\mathbb{Z}[i]$. The units of $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$, and these are the only elements with norm 1. The factorization of 2 is $2 = (1+i)(1-i) = -i(1+i)^2$, where $-i$ is a unit of $\mathbb{Z}[i]$.

Now let $p \in \mathbb{Z}_{>0}$ be an odd prime. Then $N(p) = p^2$, so if p is not irreducible in $\mathbb{Z}[i]$, then p must be the product of two irreducible elements with norm p. So if p is not irreducible, then $N(u) = a^2 + b^2 = p$ for some $u = a + bi \in \mathbb{Z}[i]$.

Siehe nächstes Blatt!

Conversely, if there is such an element u, then $p = (a+bi)(a-bi) = u\overline{u}$. So p is not irreducible if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Suppose p is not irreducible, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. If $p \mid b$, then also $p \mid a$, so $p^2 \mid a^2 + b^2 = p$, contradiction. Therefore $p \nmid b$, so there is a $c \in \mathbb{Z}$ such that $bc \equiv 1 \pmod{p}$. Then $pc^2 = (ac)^2 + (bc)^2$, so $(ac)^2 = pc^2 - (bc)^2 \equiv -1 \pmod{p}$, hence $\left(\frac{-1}{p}\right) = 1$.

Conversely, now suppose $\left(\frac{-1}{p}\right) = 1$. Then $\exists x \in \mathbb{Z}$ such that $p \mid x^2 + 1 = (x+i)(x-i)$. However $p \nmid x \pm i$, because $\frac{x \pm i}{p} = \frac{x}{p} \pm \frac{1}{p} i \notin \mathbb{Z}[i]$. So p is not a prime element of $\mathbb{Z}[i]$, and since $\mathbb{Z}[i]$ is a UFD, this means that p is not irreducible.

Summary: p is irreducible in $\mathbb{Z}[i]$ if and only if $p > 2$ and $\left(\frac{-1}{p}\right) = 1$. Moreover $p = u\overline{u}$ if $\left(\frac{-1}{p}\right) = -1$, where $u, \overline{u}$ are irreducible elements in $\mathbb{Z}[i]$.

Now we check the product formula. There is just one archemedean place of $K = \mathbb{Q}(i)$, which we denote by $|\cdot|_\infty$. Clearly $n_\infty = 2$ (non-real embedding).

If $p = 2$: The only prime ideal lying over $2 = -i(1+i)^2$ is $\mathfrak{q} = (1+i)$, and $e_{\mathfrak{q}/2} = 2$, $f_{\mathfrak{q}/2} = 1$, $n_{\mathfrak{q}/2} = 2$. So the product formula is satisfied: $|2|_\infty^2 \cdot |2|_\mathfrak{q}^2 = 2^2 \cdot (\frac{1}{2})^2 = 1$.

If $\left(\frac{-1}{p}\right) = -1$: p is irreducible, so the only prime ideal lying over p is (p), and $e_{(p)/p} = 1$, $f_{(p)/p} = 2$, $n_{(p)/p} = 2$. So the product formula is satisfied: $|p|_\infty^2 \cdot |p|_{(p)}^2 = p^2 \cdot (\frac{1}{p})^2 = 1$.

If $\left(\frac{-1}{p}\right) = 1$: $(p) = (u)(\overline{u})$, so the only prime ideals lying over p are $\mathfrak{p} = (u)$ and $\mathfrak{p}' = (\overline{u})$ (note that unlike the case $p = 2$, here $\mathfrak{p} \neq \mathfrak{p}'$), and $e_{\mathfrak{p}/p} = e_{\mathfrak{p}'/p} = 1$, $f_{\mathfrak{p}/p} = f_{\mathfrak{p}'/p} = 1$, $n_{\mathfrak{p}/p} = n_{\mathfrak{p}'/p} = 1$. So the product formula is satisfied: $|p|_\infty^2 \cdot |p|_\mathfrak{p} \cdot |p|_{\mathfrak{p}'} = p^2 \cdot \frac{1}{p} \cdot \frac{1}{p} = 1$.

d) We have the multiplicative norm $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$ on $\mathbb{Z}[\sqrt{2}]$, which is only zero for $a + bi = 0$. The units of $\mathbb{Z}[\sqrt{2}]$ are the elements with norm 1. The factorization of 2 is $2 = \sqrt{2}^2$.

Now let $p > 2$ be a prime. We claim that if $\left(\frac{2}{p}\right) = -1$, then p is irreducible in $\mathbb{Z}[\sqrt{2}]$, while if $\left(\frac{2}{p}\right) = 1$, then the decomposition of p is $p = uv$, where $u = a + b\sqrt{2}$ and $v = a - b\sqrt{2}$ are irreducible elements of $\mathbb{Z}[\sqrt{2}]$ (here $a, b \in \mathbb{Z}$).

First let $\left(\frac{2}{p}\right) = -1$, and assume indirectly that p is not irreducible. Since $N(p) = p^2$, this means that $N(a + bi) = \pm p$ for some $a, b \in \mathbb{Z}$. Then $a^2 - 2b^2 = \pm p$, so $p \nmid b$, hence $\exists c \in \mathbb{Z}$ such that $bc \equiv 1 \pmod{p}$. Then

Bitte wenden!

$(ac)^2 = \pm pc^2 + 2(bc)^2 \equiv 2 \pmod{p}$, contradicting $\left(\frac{2}{p}\right) = -1$. So p is indeed irreducible.

Now let $\left(\frac{2}{p}\right) = 1$. Then $\exists x \in \mathbb{Z}$ such that $p \mid x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. However $p \nmid x \pm \sqrt{2}$, and $\mathbb{Z}[\sqrt{2}]$ is a UFD by b), therefore p is not irreducible in $\mathbb{Z}[\sqrt{2}]$. This means that $p = uv$ for some $u, v \in \mathbb{Z}[\sqrt{2}]$ with $N(u) = N(v) = \pm p$. Since $N(1 + \sqrt{2}) = -1$, we may replace u and v by $(1 + \sqrt{2})u$ and $-(1+\sqrt{2})v$, therefore we may assume that $N(u) = p$. Then $u = a+b\sqrt{2}$ for some $a, b \in \mathbb{Z}$, and $p = N(u) = (a + b\sqrt{2})(a - b\sqrt{2})$, hence $v = a - b\sqrt{2}$.

Now we check the product formula. There are twp archemedean places of $K = \mathbb{Q}(\sqrt{2})$, corresponding to the real embeddings $\sigma_1, \sigma_2 \colon K \to \mathbb{R}$. We denote these places by $|\cdot|_\infty$ and $|\cdot|_{\infty'}$. Clearly $n_\infty = n_{\infty'} = 1$.

If $p = 2$: The only prime ideal lying over $2 = \sqrt{2}^2$ is $\mathfrak{q} = (\sqrt{2})$, and $e_{\mathfrak{q}/2} = 2$, $f_{\mathfrak{q}/2} = 1$, $n_{\mathfrak{q}/2} = 2$. So the product formula is satisfied: $|2|_\infty \cdot |2|_{\infty'} \cdot |2|_{\mathfrak{q}}^2 = 2 \cdot 2 \cdot (\frac{1}{2})^2 = 1$.

If $p > 2$ and $\left(\frac{2}{p}\right) = -1$: p is irreducible, so the only prime ideal lying over p is (p), and $e_{(p)/p} = 1$, $f_{(p)/p} = 2$, $n_{(p)/p} = 2$. So the product formula is satisfied: $|p|_\infty \cdot |p|_{\infty'} \cdot |p|_{(p)}^2 = p \cdot p \cdot (\frac{1}{p})^2 = 1$.

If $p > 2$ and $\left(\frac{2}{p}\right) = 1$: $(p) = (u)(v)$, so the only prime ideals lying over p are $\mathfrak{p} = (u)$ and $\mathfrak{p}' = (v)$ (it is easy to see that $\frac{u}{v} = \frac{u^2}{p} \notin \mathbb{Z}[\sqrt{2}]$, so $(u) \neq (v)$), and $e_{\mathfrak{p}/p} = e_{\mathfrak{p}'/p} = 1$, $f_{\mathfrak{p}/p} = f_{\mathfrak{p}'/p} = 1$, $n_{\mathfrak{p}/p} = n_{\mathfrak{p}'/p} = 1$. So the product formula is satisfied: $|p|_\infty \cdot |p|_{\infty'} \cdot |p|_{\mathfrak{p}} \cdot |p|_{\mathfrak{p}'} = p \cdot p \cdot \frac{1}{p} \cdot \frac{1}{p} = 1$.