ALGEBRAIC NUMBER THEORY

MIDTERM 1

(1) Find the fundamental unit of $\mathbb{Q}(\sqrt{6}\,)$.

The fundamental unit comes from the smallest positive solution of the corresponding Pell equation. Since $6 \equiv 2 \bmod 4$, we need to solve $x^2 - 6y^2 = \pm 1$. The smallest positive solution is $(5, 2)$, hence $\varepsilon = 5 + 2\sqrt{6}$ is the fundamental unit.

Remark. Of course you can also compute the unit using elements of small norm, but then you have to check that the unit you find is fundamental. These were supposed to be 20 pts for free.

(2) Show that $10 = 2 \cdot 5 = -\sqrt{-10} \cdot \sqrt{-10}$ is an example of nonunique factorization in $\mathbb{Z}[\sqrt{-10}\,]$, and show also how this factorization can be explained in terms of unique factorization into prime ideals.

We first have to show that the factors are irreducible and do not differ by units. Assume that $2 = \alpha\beta$; then $4 = N(2) = N\alpha N\beta$. Since $N\alpha = \pm 2$ does not have a solution ($x^2 + 10y^2 = \pm 2$ is clearly impossible). Thus $N\alpha = \pm 1$ or $N\beta = \pm 1$, which shows that α or β is a unit, hence 2 is irreducible. The same argument works for the other factors.

Since the only units are ± 1, the factors obviously do not differ just by a unit.

Explanation via ideal theory: Since 2 and 5 divide the discriminant, there are only two ideals involved here, namely $\mathfrak{p} = (2, \sqrt{-10}\,)$ and $\mathfrak{q} = (5, \sqrt{-10}\,)$; clearly $\mathfrak{p}^2 = (2)$ and $\mathfrak{p}^2 = (5)$, as well as $\mathfrak{pq} = (\sqrt{-10}\,)$. Thus the different factorizations above can be explained by the ideal factorization $(10) = \mathfrak{p}^2 \cdot \mathfrak{q}^2 = (\mathfrak{pq})^2$.

(3) Let $p \equiv 3 \bmod 4$ be prime. Show that exactly one of the two equations $a^2 - 2pb^2 = 2$ or $a^2 - 2pb^2 = -2$ is solvable in integers.

Start with a minimal positive solution of $x^2 - 2py^2 = 1$. Clearly x is odd. Now $2py^2 = x^2 - 1 = (x-1)(x+1)$. The factors on the right have gcd equal to 2 (their difference is 2, so it cannot be any bigger; it is at least 2 since $x \pm 1$ are both even). Thus $x - 1 = 2ar^2$, $x + 1 = 2bs^2$ with $ab = 2p$

and $y = 2rs$, giving rise to four possible sets of equations:

$$\begin{aligned} x-1 &= 2r^2 & \qquad x+1 &= 4ps^2, \\ x-1 &= 4r^2 & \qquad x+1 &= 2ps^2, \\ x-1 &= 2pr^2 & \qquad x+1 &= 4s^2, \\ x-1 &= 4pr^2 & \qquad x+1 &= 2s^2. \end{aligned}$$

Subtracting these equations from each other and dividing through by 2 shows that one of the following equations must hold:

$$\begin{aligned} 1 &= 2ps^2 - r^2, \\ 1 &= ps^2 - 2r^2, \\ 1 &= 2s^2 - pr^2, \\ 1 &= s^2 - 2pr^2. \end{aligned}$$

The last equation contradicts the minimality of y because $y = 2rs$ shows that $0 < |r| < y$. The first equation does not hold modulo 8: since $p \equiv 3 \bmod 4$, we have $2p \equiv 6 \bmod 8$; moreover, r is odd, hence we find $1 = 2ps^2 - r^2 \equiv 6s^2 - 1 \bmod 8$ or $6s^2 \equiv 2 \bmod 8$. But this congruence is not solvable. Alternatively, reducing the equation modulo p shows that $-1 \equiv r^2 \bmod p$, which is impossible for primes $p \equiv 3 \bmod 4$.

We have proved that one of the equations $2x^2 - py^2 = \pm 1$ are solvable. Multiplying through by 2 proves that one of $(2x)^2 - 2py^2 = \pm 2$ is solvable.

It remains to show that at most one of them has a solution in integers. But the equation $a^2 - 2pb^2 = 2$ implies $(\frac{2}{p}) = +1$, i.e., $p \equiv 7 \bmod 8$, whereas $a^2 - 2pb^2 = -2$ implies $(\frac{-2}{p}) = +1$, i.e., $p \equiv 3 \bmod 8$.

(4) Write down all prime ideals of norm ≤ 11 in $K = \mathbb{Q}(\sqrt{103}\,)$ (No proofs required, but your list should be correct and complete). Also find the prime ideal factorization of $(13 + \sqrt{103}\,)$.

The zero ideal (0) is a prime ideal; the unit ideal (1) is not prime. Since 103 is a prime $\equiv 3 \bmod 4$, among the primes ≤ 11 only 2 is ramified, and we have $(2) = \mathfrak{p}_2^2$ for the prime ideal $\mathfrak{p}_2 = (2, 1 + \sqrt{103}\,)$ of norm 2.

The odd primes ≤ 11 are either split or inert. We compute the Legendre symbols to find out which: $(\frac{103}{3}) = +1$, $(\frac{103}{5}) = (\frac{103}{7}) = -1$, and $(\frac{103}{11}) = +1$ show that (5) and (7) are inert (of norms 25 and 49, respectively), and that 3 and 11 split.

Now $103 \equiv 1^2 \bmod 3$ shows that the two prime ideals of norm 3 are $\mathfrak{p}_3 = (3, 1 + \sqrt{103}\,)$ and its conjugate $\mathfrak{p}_3'$. Next $103 \equiv 4 \equiv 2^2 \bmod 11$ shows that $\mathfrak{p}_{11} = (11, 2 + \sqrt{103}\,)$ and its conjugate are the prime ideals of norm 11. Thus our complete list of prime ideals of norm ≤ 11 is $(0), \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_{11}, \mathfrak{p}_{11}'$.

Remarks. Some of you seem to be convinced that prime ideals have to have the form $(p, 1 + \sqrt{m}\,)$. This is nonsense. Of course we can form the ideal $(5, 1 + \sqrt{103}\,)$, but it contains 5 and $(1 + \sqrt{103}\,)(1 - \sqrt{103}\,) = -102$, hence it also contains $\gcd(5, 102) = 1$ and so is the unit ideal.

You can also form the $\mathbb{Z}$-module $[5, 1 + \sqrt{103}\,]$; but this is not an ideal, as you will easily check.

(5) Find the prime ideal factorizations of $(7+\sqrt{103}\,)$ and $(10+\sqrt{103}\,)$, and use this to write down an expression for a unit $\varepsilon > 1$ in $\mathcal{O}_K$ (you need not show that this unit is fundamental).

We find $N(7+\sqrt{103}\,) = -54 = -2\cdot 3^3$ and $N(10+\sqrt{103}\,) = -3$. Since $10+\sqrt{103} \equiv 7+\sqrt{103} \equiv 1+\sqrt{103} \bmod 3$ and $1+\sqrt{103} \in \mathfrak{p}_3$, we have $(7+\sqrt{103}\,) = \mathfrak{p}_2\mathfrak{p}_3^3$ and $(10+\sqrt{103}\,) = \mathfrak{p}_3$. Thus $\alpha = \frac{7+\sqrt{103}}{(10+\sqrt{103}\,)^3}$ generates $\mathfrak{p}$, and from $\mathfrak{p}^2 = (2)$ we now see that $\varepsilon = \frac{1}{2}\alpha^2$ is a nontrivial positive unit. If we should have $\varepsilon < 1$, then $1/\varepsilon$ is a unit > 1.

Oh, and by using the formulation "write down an expression" I was hoping to convey the idea that you do not have to write down a numerical expression such as $\varepsilon = 227528 + 22419\sqrt{103}$.