ALGEBRAIC NUMBER THEORY

MIDTERM 2

(1) Let R be a domain, and let $a, b, c \in R$ be elements with $(a, b) = 1$. Show that $(a, bc) = (a, c)$.

I meant to write $(a, b) = (1)$; in any case it should be clear that in general domains, gcd's need not exist. This means that you are not allowed to assume that $(a, c) = (d)$ is principal.

Clearly $(a, bc) \subseteq (a, c)$. For showing the converse, observe that there are $r, s \in R$ with $ar + bs = 1$. Multiplying through by c gives $c = acr + bcs$, hence $c \in (a, bc)$. Thus $a \in (a, bc)$ and $c \in (a, bc)$.

Here's a different proof: we have

$$(a, c) = (a, b)(a, c) = (a^2, ab, ac, bc) \subseteq (a, bc).$$

(2) Show that $10 = 2 \cdot 5 = -\sqrt{-10} \cdot \sqrt{-10}$ is an example of nonunique factorization in $R = \mathbb{Z}[\sqrt{-10}\,]$.

Since the only units in R are ± 1, the factors do not differ by units. We claim that 2 is irreducible. In fact, assume that $2 = \alpha\beta$; taking norms gives $4 = N\alpha N\beta$.

If $N\alpha = 2$ for $\alpha = a + b\sqrt{-10}$, then $a^2 + 10b^2 = 2$: contradiction. Thus $N\alpha = 1$ or $N\beta = 1$, and this implies that α or β is a unit. This means that 2 is irreducible.

Now $2 \mid \sqrt{10} \cdot \sqrt{10}$, but $2 \nmid \sqrt{10}$; this implies that 2 is not prime. But since irreducibles are primes in UFDs, the domain $\mathbb{Z}[\sqrt{10}\,]$ cannot be a UFD.

(3) Find the prime ideal factorizations of (2) and $(\frac{1+\sqrt{17}}{2})$ in $\mathbb{Q}(\sqrt{17}\,)$.

We have $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ with $\mathfrak{p}_2 = (2, \omega)$ and $\omega = \frac{1+\sqrt{17}}{2}$. Since $N\omega = -4$, the ideal (ω) is one of $\mathfrak{p}_2^2$, $(\mathfrak{p}_2')^2$ or $\mathfrak{p}_2\mathfrak{p}_2' = (2)$. The last case is impossible, since ω is not divisible by 2. Since $\omega \in \mathfrak{p}_2$, we must have $(\omega) = \mathfrak{p}_2^2$.

(4) Let $p \equiv 3 \bmod 4$ be a prime, and let (t, u) be a positive solution of the Pell equation $t^2 - pu^2 = 1$. Show that if u is even, then $t + u\sqrt{p}$ is a square in $\mathbb{Q}(\sqrt{p}\,)$.

Hint: show that there must be a "smaller" solution (a, b) of the Pell equation and consider $a + b\sqrt{p}$.

We have $pu^2 = (t-1)(t+1)$. Since $2 \mid u$, t is odd, and we easily find $\gcd(t-1, t+1) = 2$. But then $t+1 = 2a^2, t-1 = 2pb^2$ or $t+1 = 2pa^2, t-1 = 2b^2$. The second case leads to $n^2 - pa^2 = -1$, which gives $b^2 \equiv -1 \bmod p$:

contradiction. Thus we are in the first case and have $a^2 - pb^2 = 1$. Note that $a^2 + pb^2 = t$ and $u = 2ab$. But then $(a + b\sqrt{p}\,)^2 = t + u\sqrt{p}$.

(5) Let p be an odd prime, m a squarefree integer not divisible by p, and assume that $m \equiv x^2 \bmod p$. Show that $\mathfrak{p}\mathfrak{p}' = (p)$ for the ideals $\mathfrak{p} = (p, x + \sqrt{m}\,)$ and $\mathfrak{p}' = (p, x - \sqrt{m}\,)$.

Write $x^2 - m = pt$; then we have

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= (p, x + \sqrt{m}\,)(p, x - \sqrt{m}\,) \\ &= (p^2, p(x + \sqrt{m}\,), p(x - \sqrt{m}\,), x^2 - m) \\ &= (p)(p, x + \sqrt{m}, x - \sqrt{m}, t). \end{aligned}$$

Now there are two cases:
(a) $p \mid x$. Then $p \nmid t$, hence the second ideal contains the coprie elements p and t, hence is the unit ideal.
(b) $p \nmid x$: then the second ideal contains p and $2x$, hence 1.
Thus $\mathfrak{p}\mathfrak{p}' = (p)$ in both cases.

(6) Consider the quadratic number field $K = \mathbb{Q}(\sqrt{46}\,)$.
(a) List all prime ideals in $\mathcal{O}_K$ with norm ≤ 7. We have $\operatorname{disc} K = -4 \cdot 46$.

Thus $(2) = \mathfrak{p}_2^2$ for $\mathfrak{p}_2 = (2, \sqrt{46}\,)$. Moreover, $46 \equiv 1^2 \bmod 3$ and $46 \equiv 1^2 \bmod 5$ and $46 \equiv 2^2 \bmod 7$ shows that the primes 3, 5 and 7 split. We find $\mathfrak{p}_3 = (3, 1 + \sqrt{46}\,)$, $\mathfrak{p}_5 = (5, 1 + \sqrt{46}\,)$, and $\mathfrak{p}_7 = (7, 2 + \sqrt{46}\,)$.

(b) Find the prime ideal factorizations of $(2 + \sqrt{46}\,)$, $(7 + \sqrt{46}\,)$ and $(8 + \sqrt{46}\,)$.

$(2 + \sqrt{46}\,) = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_7$; $(7 + \sqrt{46}\,) = \mathfrak{p}_3$; $(8 + \sqrt{46}\,) = \mathfrak{p}_2{\mathfrak{p}_3'}^2$.

(c) Find a unit $\varepsilon > 1$ in $\mathcal{O}_K$. Clearly $\alpha = \frac{8+\sqrt{46}}{(7-\sqrt{46}\,)^2}$ generates $\mathfrak{p}_2$. Since

$(2) = \mathfrak{p}_2^2$, the element $\varepsilon = \frac{1}{2}\alpha^2$ must be a unit. Since 2 is not a square in K, ε cannot be trivial.

(d) Explain how to show that your ε is fundamental (no calculations; just explain the method). Assume that $1 < \varepsilon = \eta^m$. Then $m \le \frac{\log \varepsilon}{\log \sqrt{46}}$.

Test all possible m (check the notes for detail).

(e) Show that K has class number 1.

The Gauss bound is $\mu_K = \sqrt{4 \cdot 46/5} < 7$; thus we need to show that all ideals with norm < 7 are principal. We already know that $\mathfrak{p}_2 = (\alpha)$ and $\mathfrak{p}_3 = (7 + \sqrt{46}\,)$ as well as $\mathfrak{p}_3'$ are principal. The factorization $(6 + \sqrt{46}\,) = \mathfrak{p}_2\mathfrak{p}_5$ shows that $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ are principal. Finally it follows from $(2 + \sqrt{46}\,) = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_7$ that $\mathfrak{p}_7$ and $\mathfrak{p}_7'$ are principal.

Note that the Gauss bound tells us something about ideals in certain ideal classes. It most certainly does not claim that all ideals have norm $< \mu_K$.

(7) Compute the ideal class group of $K = \mathbb{Q}(\sqrt{-33})$.

We have disc $K = -4{\cdot}33$, hence the Gauss bound is $\mu_K = \sqrt{4 \cdot 33/3} < 7$. We find $(2) = \mathfrak{p}_2^2$ for $\mathfrak{p}_2 = (2, 1+\sqrt{-33})$; $(3) = \mathfrak{p}_3^2$ for $\mathfrak{p}_3 = (3, \sqrt{-33})$; $(\frac{-33}{5}) = -1$, so 5 is inert; $-33 \equiv 2 \equiv 3^2 \bmod 7$ gives $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ for $\mathfrak{p}_7 = (7, 3+\sqrt{-33})$.

Now we claim that the ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\mathfrak{p}_7$ and $\mathfrak{p}_3\mathfrak{p}_7$ are not principal. This follows from the fact that the equations $x^2 + 33y^2 = 2, 3, 7, 6, 14, 21$ do not have integral solutions. This proves that the four ideal classes $[(1)]$, $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_2\mathfrak{p}_3]$ are pairwise distinct. Moreover, they all have order dividing 2: this is clear from $\mathfrak{p}_2^2 = (2)$nd $\mathfrak{p}_3^2 = (3)$.

Now $(3+\sqrt{-33}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ shows that $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7 \sim 1$; multiplying through by $\mathfrak{p}_2\mathfrak{p}_3$ shows that $\mathfrak{p}_7 \sim \mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_7 \sim \mathfrak{p}_2\mathfrak{p}_3$. Taking conjugates gives $\mathfrak{p}_7 \sim \mathfrak{p}_2\mathfrak{p}_3$.

Thus $\mathrm{Cl}(K) = \{[(1)], [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_2\mathfrak{p}_3]\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.