END OF SEMESTER EXAM, MP473, 1992

Time: Three hours
Candidates should aim to complete SIX questions, but may attempt as many questions as they wish.

(In what follows, $A(\sqrt{d})$ denotes the ring of integers in $\mathbb{Q}(\sqrt{d})$.)

1. (a) Define the term algebraic integer and prove that a complex number $\theta$ is an algebraic integer if and only if $\exists w_1, \ldots, w_n$, not all zero, such that for $1 \leq i \leq n,$

$$w_i \theta = \sum_{j=1}^{n} a_{ij} w_j,$$

where $a_{ij} \in \mathbb{Z}$ for $1 \leq i \leq n, 1 \leq j \leq n.$

(b) If $\theta$ is an algebraic integer and is also a rational number, prove that $\theta$ is an integer.

(c) Prove that the sum and product of two algebraic integers is also an algebraic integer.

2. (a) Prove that the ring $\mathbb{Z}[i]$ of Gaussian integers is Euclidean.

(b) Determine the units of $\mathbb{Z}[i].$

(c) Describe the factorization of a prime $p$ into irreducibles of $\mathbb{Z}[i].$

(d) Determine the factorization of $6 + 7i$ into irreducibles of $\mathbb{Z}[i].$

3. (a) If $k$ is an odd rational integer, prove that

$$\gcd (k + i, k - i) = 1 + i.$$  

(b) Show that the only solutions of the Diophantine equation

$$x^2 + 1 = 2y^3$$

are $x = \pm 1, y = 1.$

4. An integer $\alpha > 0$ of $\mathbb{Q}(\sqrt{d}),$ $d > 0,$ is called primary if

$$1 \leq \left| \frac{\alpha}{\sigma(\alpha)} \right| < \eta^2,$$

where $\eta$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$. 

1
(a) Prove that every non-zero integer of \( \mathbb{Q}(\sqrt{d}) \) is the associate of precisely one primary integer.

(b) Prove that the primary integers \( \alpha \) with \( N(\alpha) = n \) satisfy

\[
\alpha^2 - A\alpha + n = 0,
\]

where \( |A| < \sqrt{|n|}(1 + \eta) \).

(c) Find the primary integers of \( \mathbb{Q}(\sqrt{2}) \) with norm equal to 7 and hence find all solutions in integers of \( x^2 - 2y^2 = 7 \).

5. (a) If \( p \) is a prime of the form \( 3n + 1 \), use the fact that the integers of \( \mathbb{Q}(\sqrt{-3}) \) form a UFD to prove that \( p = x^2 - xy + y^2 \) is soluble in integers \( x \) and \( y \). How many solutions are there?

(b) If \( p \) is a prime of the form \( 8n \pm 1 \), use the fact that the integers of \( \mathbb{Q}(\sqrt{2}) \) form a UFD to prove that \( p = x^2 - 2y^2 \) is soluble in integers \( x \) and \( y \). (Hint: \( \eta = 1 + \sqrt{2} \) is the fundamental unit and \( N(\eta) = -1 \).

6. (a) Prove Hurwitz’ lemma: Let \( \alpha, \beta \in A(\sqrt{d}) \), \( g|N(\alpha) \), \( g|N(\beta) \), \( g|(\alpha\sigma(\beta) + \beta\sigma(\alpha)) \), where \( \sigma(\alpha) \) is the conjugate of \( \alpha \). Prove that \( g|\alpha\sigma(\beta) \).

(HINT: \( \xi = \alpha\sigma(\beta) \) satisfies the equation

\[
\xi^2 - T(\xi)\xi + N(\xi) = 0.
\]

(b) Use Hurwitz’ lemma to prove that if \( A \) is an ideal of \( A(\sqrt{d}) \), then

\[
A\sigma(A) = (g),
\]

where \( g \in \mathbb{N} \).

(c) Also prove that if \( A \) and \( C \) are ideals in \( A(\sqrt{d}) \), then

\[
A|C \iff A \supseteq C.
\]

7. Let \( p \) be a prime, \( d \) a squarefree integer, \( \omega = (1 + \sqrt{d})/2 \) if \( d \equiv 1 \) (mod 4), but \( \sqrt{d} \) otherwise. Also let \( f \) be the defining polynomial of \( \omega \). Let \( A = (p, a + \omega) \), where \( a \in \mathbb{Z} \).

(a) Prove that \( A = (1) \) if \( f(-a) \not\equiv 0 \) (mod \( p \)).

(HINT: \( \gcd(x + a, f) = 1 \) in \( \mathbb{Z}_p[x] \).)
(b) If \( f(-a) \equiv 0 \pmod{p} \), prove directly that \( N(A) = p \) by showing that the integers \( 0, \ldots, p-1 \) form a complete set of representatives \((\text{mod } A)\).  
(HINT: (1) Write \( \omega = -a + (\omega + a) \); (2) Use the fact that \( f = (x + a)(x + b) \) in \( \mathbb{Z}_p[x] \) for some \( b \in \mathbb{Z} \) so that \((\omega + a)(\omega + b) \equiv 0 \pmod{p} \).

(c) Suppose that \( f = (x + a)(x + b) \) in \( \mathbb{Z}_p[x] \). Prove that  
\( (p) = (p, a + \omega)(p, b + \omega) \).
(HINT: Use the fact that \( N((p)) = p^2 \)).

(d) If \( f \) is irreducible in \( \mathbb{Z}_p[x] \), prove that \( (p) \) is a prime ideal.

(e) If \( d = -23 \), find the prime ideal decomposition of \((\omega - 2)\).
(HINT: Find \( N(\omega - 2)\)).

8. (a) Define the Kronecker symbol \((\frac{\Delta}{k})\), where \( \Delta \) is a fundamental discriminant and \( k \in \mathbb{N} \).

(b) Let \( m \in \mathbb{N} \) and \( \gcd(\Delta, m) = 1 \), where \( \Delta \) is an odd fundamental discriminant. Prove that  
\[ \left( \frac{\Delta}{m} \right) = \left( \frac{m}{|\Delta|} \right) \, , \]
where the right hand side is a Jacobi symbol. (HINT: write \( m = 2^l w \), \( w \) odd.)

(c) Let  
\[ G(\Delta) = \sum_{k=1}^{|\Delta|} \left( \frac{\Delta}{k} \right) e^{2\pi i k / |\Delta|} \, , \]

(i) Verify directly that \( G(5) = \sqrt{5} \).
(ii) Prove that if \( p \) is an odd prime and \( p^* = (-1)^{\frac{p-1}{2}} \), then  
\[ G(p^*) = \sum_{k=0}^{p-1} e^{2\pi i k^2 / p} \, , \]
and deduce that  
\[ G^2(p^*) = p^* \, . \]
9. (a) Find the group structure of the multiplicative group of equivalence classes of ideals in \( A(\sqrt{-21}) \).

(b) Let \( d > 0 \) and squarefree, \((\alpha) = A^2\), where \( A \) is an ideal in \( A(\sqrt{d})\), \( N(\alpha) < 0 \) and \( N(\eta) = 1 \), where \( \eta \) is the fundamental unit. Prove that \( A \) is not principal.

(c) Consider the ideal \( A = (3, 1 + \sqrt{34}) \). Prove that \( A^2 = (-5 + \sqrt{34}) \) and hence prove that \( A \) is not principal, given that \( 35 + 6\sqrt{34} \) is the fundamental unit of \( \mathbb{Q}(\sqrt{34}) \).

10. Let \( m > 0 \) and squarefree.

(a) Prove that \( A(\sqrt{-m}) \) is not a UFD if one of the following hold:
   (i) \( m \equiv 1 \pmod{4}, m > 1 \);
   (ii) \( m \equiv 2 \pmod{4}, m > 2 \);
   (iii) \( m \equiv 7 \pmod{8}, m > 7 \).

(b) If \( A(\sqrt{-m}) \) is a UFD and \( m \equiv 3 \pmod{8} \), prove that \( m \) is a prime and that \( x^2 + x + \frac{m+1}{4} \) assumes prime values for \( x = 0, 1, \ldots, \frac{m-3}{4} \). (These are Euler’s prime–producing polynomials.)

(c) Suppose that \( m \equiv 3 \pmod{8} \), \( m \) is a prime and that \( x^2 + x + \frac{m+1}{4} \) assumes prime values for \( x = 0, 1, \ldots, \frac{m-3}{4} \). Prove that \( A(\sqrt{-m}) \) is a UFD by showing that all ideals are principal.

11. Do one of the following only:

(a) Use the Gaussian sum identity \( G(\Delta) = \sqrt{\Delta} \) to explicitly evaluate the series
\[
\sum_{n=1}^{\infty} \left( \frac{\Delta}{n} \right) \frac{1}{n}.
\]

(b) Sketch a proof of the formula \( G(p^*) = \sqrt{p^*} \), where \( p \) is an odd prime and \( p^* = (-1)^{\frac{p-1}{2}} p \).