EXAMPLE SHEET

NUMBER FIELDS

Mich. Term 1995
Prof. A. Baker

1. Find the minimum polynomials over $\mathbb{Q}$ of $(1+i)\sqrt{3}, i+\sqrt{3}, i+e^{i\pi/3}$.

2. Find the field polynomials of i and $\sqrt[3]{5}$ in $\mathbb{Q}(i+\sqrt[3]{5})$.

3. By the symmetric function theorem, or otherwise, prove that any zero of a monic polynomial $p(x)$ with algebraic integer coefficients is an algebraic integer.

4. Which of the following are algebraic integers?

$$1/2, (\sqrt{3}+\sqrt{5})/2, (\sqrt{3}+\sqrt{7})/\sqrt{2}, (1+\sqrt[3]{10}+\sqrt[3]{100})/3.$$

5. Explain why the equation

$$2.11 = (5+\sqrt{3})(5-\sqrt{3})$$

is not inconsistent with the fact that $\mathbb{Q}(\sqrt{3})$ has unique factorisation.

6. Find equations to show that $\mathbb{Q}(\sqrt{d})$ does not have unique factorisation for $d = -10, -13, -14$ and -15.

7. What is the Galois group of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are distinct primes?

Find an integral basis for the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Calculate the discriminant of the field.

8. Let d be a square-free integer not divisible by 3, and let $\delta = \sqrt[3]{d}$. Show that $\Delta(1, \delta, \delta^2) = -27d^2$.

Let $\alpha = u + v\delta + w\delta^2$ be the general element of $\mathbb{Q}(\delta)$ with u, v, w rational. Calculate the norm of $\alpha - u$ and the traces of α, $\alpha\delta$, $\alpha\delta^2$.

Hence, or otherwise, show that if $d \not\equiv \pm 1 \pmod 9$ then $1, \delta, \delta^2$ is an integral basis for $\mathbb{Q}(\delta)$.

9. Find single generators for the ideals $[2613, 2171]$ in $\mathbb{Z}$ and $[51-5i, 43+7i]$ in the Gaussian field $\mathbb{Q}(i)$.

10. Factorise the ideals $[2]$ and $[6]$ in the field $\mathbb{Q}(\sqrt{-6})$ into a product of prime ideals. Similarly factorise $[5]$ in $\mathbb{Q}(\sqrt[3]{3})$ and $[13]$ in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

11. Find the fundamental unit in $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$.

12. Describe all the integers solutions of the equations

$$x^2 - 2y^2 = 1, \quad x^2 - 3y^2 = -1, \quad x^2 - 5y^2 = -1.$$

13. Show that $\mathbb{Q}(\sqrt{5})$ has class number 1.
Describe all the integer solutions of the equations

$$x^2 - 5y^2 = 7, \quad x^2 - 5y^2 = 11, \quad x^2 - 5y^2 = 121.$$

14. Show that $\mathbb{Q}(\sqrt{7})$ has class number 1 and find a fundamental unit.
Describe all the integer solutions of the equations

$$x^2 - 7y^2 = 2, \quad x^2 - 7y^2 = 13.$$

15. For which primes p is the equation $x^2 + 13y^2 = p$ soluble in integers?

16. Establish the following facts about the factorisation of principal ideals in $\mathbb{Q}(\sqrt{-d})$ where d is a positive square-free integer.

(i) If d is composite and p is an odd prime divisor of d then $[p] = \wp^2$ where $\wp$ is not principal.

(ii) If $d \equiv 1$ or $2 (\mathrm{mod}\, 4)$ then $[2] = \wp^2$ where $\wp$ is not principal unless $d = 1$ or 2.

(iii) If $d \equiv 7 (\mathrm{mod}\, 8)$ then $[2] = \wp\overline{\wp}$ where $\wp$ is not principal unless $d = 7$.

Hence show that if $\mathbb{Q}(\sqrt{-d})$ has class number 1 then either $d = 1$, 2 or 7, or d is prime and $d \equiv 3 (\mathrm{mod}\, 8)$.

17. Show that $\mathbb{Q}(\sqrt{-d})$ has class number 1 for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ [These are in fact the only values].

18. Find the class group of $\mathbb{Q}(\alpha)$, where α is

$$\sqrt{-6}, \sqrt{-29}, \sqrt{79}, \sqrt[3]{2}, \sqrt[3]{7}, e^{2\pi i/5}.$$

19. Find the class group of $\mathbb{Q}(\sqrt{-6}, \sqrt{2})$.
Determine how a prime ideal in the subfield $\mathbb{Q}(\sqrt{-6})$ factorises into prime ideals in the field itself.

TYPICAL TRIPOS QUESTIONS: NUMBER FIELDS

[1992] Factorise (2) in the ring of integers of $\mathbb{Q}(\sqrt{65})$. Show that the primes dividing (2) are not principal. Find the ideal class group of $\mathbb{Q}(\sqrt{65})$.

Describe all integer solutions of $X^2 - 65Y^2 = 40$.

[1992] Find the discriminant of $\mathbb{Q}(\sqrt[3]{2})$. [You may assume that $\mathbb{Z}[\sqrt[3]{2}]$ is the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$].

Find the norm of the principal ideal $(a + b\sqrt[3]{2} + c\sqrt[3]{4})$ in $\mathbb{Z}[\sqrt[3]{2}]$. Show that $1 - 2\sqrt[3]{2} + \sqrt[3]{4}$ is a unit in $\mathbb{Z}[\sqrt[3]{2}]$. How many integer solutions do the Diophantine equations $X^3 + 2Y^3 + 4Z^3 - 6XYZ = n$ have for $n = 1, -1, 2$ and 7?

[1993] Factorise the ideals (2), (5), $(1 + \sqrt{-26})$ and $(2 + \sqrt{-26})$ in the ring of integers of $\mathbb{Q}(\sqrt{-26})$. Find the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{-26})$.

[1993] Write an essay on factorisation in number fields and applications to Diophantine equations. [Your account need not be exhaustive].

[1994] Factorise the ideals (2), (3) and $(2 + \sqrt{-14})$ in the ring of integers of $\mathbb{Q}(\sqrt{-14})$. Find the class group of the ring of integers of $\mathbb{Q}(\sqrt{-14})$.

[1994] Find a fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{10})$.

Describe all integer solutions of the equation $x^2 - 10y^2 = n$ for $n = -1, 6$ and 7.

[1994,III] State Dedekind's theorem on the ideal factorisation of rational primes in fields k with a power integral basis. Briefly outline the proof.

Determine how the primes 2 and 5 factorise in $\mathbb{Q}(\varsigma)$, where $\varsigma = e^{2\pi i/5}$. [It can be assumed that $\mathbb{Q}(\varsigma)$ has an integral basis $1, \varsigma, \varsigma^2, \varsigma^3$].

[1995] State Dedekind's theorem on the ideal factorisation of rational primes in fields k with a power integral basis. Find the ideal class group of the quadratic field $k = \mathbb{Q}(\sqrt{-22})$. [It can be assumed that every ideal in k is equivalent to one with norm at most $(2/\pi)\sqrt{|d|}$, where d is the discriminant of k.]

[1995] State Dirichlet's theorem on the units of an algebraic number field k. State also a simplified version in the case of a real quadratic field.

Show that there are only finitely many ideals in k with a given norm m. Hence verify that there are only finitely many non-associated elements in the ring of integers of k with norm m.

What does this tell us about the general form of the solutions, if any, of the equation

$$x^2 - dy^2 = m$$

in integers x, y, where d is a positive integer?

[1995] Explain what is meant by a *basis* $\gamma_1, ..., \gamma_n$ of an ideal in a number field k. Define the *discriminant* $\Delta = \Delta(\gamma_1, ..., \gamma_n)$ and state the fundamental property of Δ when $\gamma_1, ...\gamma_n$ is a basis. Hence prove that every ideal in k has a basis.

Write down a formula for the norm of an ideal in terms of Δ and the discriminant of k. Show that the norm of the principal ideal generated by α is given by $|N\alpha|$, where N is the field norm of k. Show further that the norm of a prime ideal has the form p^f for some rational prime p and integer f.

Prove that if

$$\gamma_i = u_{i1}\omega_1 + ... + u_{in}\omega_n \quad (1 \leqslant i \leqslant n),$$

where $\omega_1, ..., \omega_n$ is an integral basis for k and the u_{ij} are rational integers, then the norm of the ideal with basis $\gamma_1, ..., \gamma_n$ is given by $|\det u_{ij}|$.