Lent Term 2016

Number Fields: Example Sheet 1 of 3

1. Find the minimal polynomials over $\mathbb{Q}$ of
$$(1+i)\sqrt{3}, \qquad i+\sqrt{3}, \qquad 2\cos(2\pi/7).$$

2. Which of the following are algebraic integers?
$$\sqrt{5}/\sqrt{2}, \ \ (1+\sqrt{3})/2, \ \ (\sqrt{3}+\sqrt{7})/2, \ \ \frac{3+2\sqrt{6}}{1-\sqrt{6}}, \ \ (1+\sqrt[3]{10}+\sqrt[3]{100})/3, \ \ 2\cos(2\pi/19).$$

3. Let $d>1$ be an integer. Show that the only units in the ring
$$\mathbb{Z}[\sqrt{-d}] = \{a+b\sqrt{-d} : a,b \in \mathbb{Z}\}$$
are ± 1.

4. (i) Explain why the equations
$$2 \cdot 11 = (5+\sqrt{3})(5-\sqrt{3})$$
and
$$(2+\sqrt{7})(3-2\sqrt{7}) = (5-2\sqrt{7})(18+7\sqrt{7})$$
are not inconsistent with the fact $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$ have unique factorisation.
(ii) Find equations to show that $\mathbb{Z}[\sqrt{d}]$ is not a UFD for $d=-10,-13,-14$.

5. Let K be a field with $\mathrm{char}(K) \neq 2$. Show that every extension L/K of degree 2 is of the form $L=K(\sqrt{a})$ with $a \in K^*$, $a \notin (K^*)^2$. Show further that $K(\sqrt{a})=K(\sqrt{b})$ if and only if $a/b \in (K^*)^2$.

6. Let $A \subseteq B \subseteq C$ be rings.
(i) Show that if B is finite over A, and C is finite over B, then C is finite over A.
(ii) Show that if B is integral over A, and C is integral over B, then C is integral over A.

Now let $\mathbb{Q} \subseteq K \subseteq L$ be finite extensions of fields.
(i) Show that if $\alpha \in L$ is integral over $\mathcal{O}_K$ it is an algebraic integer.
(ii) Show that if $f \in K[x]$ is monic, and $f^n \in \mathcal{O}_K[x]$ for some n, then $f \in \mathcal{O}_K[x]$.

7. Let $K=\mathbb{Q}(\theta)$ where θ is a root of X^3-2X+6. Show that $[K:\mathbb{Q}]=3$ and compute $N_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ for $\alpha = n-\theta$, $n \in \mathbb{Z}$ and $\alpha = 1-\theta^2, 1-\theta^3$.

8. Let $K=\mathbb{Q}(\delta)$ where $\delta = \sqrt[3]{d}$ and $d \neq 0, \pm 1$ is a square-free integer. Show that $\Delta(1,\delta,\delta^2) = -27d^2$. By calculating the traces of θ, $\delta\theta$, $\delta^2\theta$, and the norm of θ, where $\theta = u+v\delta+w\delta^2$ with $u,v,w \in \mathbb{Q}$, show that the ring of integers $\mathcal{O}_K$ of K satisfies
$$\mathbb{Z}[\delta] \subset \mathcal{O}_K \subset \tfrac{1}{3}\mathbb{Z}[\delta].$$

9. Let $K = \mathbb{Q}(\alpha)$ be a number field. Suppose $\alpha \in \mathcal{O}_K$ and let $f \in \mathbb{Z}[X]$ be its minimal polynomial.

   (i) Show that if the discriminant of f is a square-free integer then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

   (ii) Compute an integral basis for K in the cases $f(X) = X^3 + X + 1$ and $f(X) = X^3 - X - 4$.

   [*The discriminant of* $X^3 + aX + b$ *is* $-4a^3 - 27b^2$.]

10. Let $K = \mathbb{Q}(i, \sqrt{2})$. By computing the relative traces $\mathrm{Tr}_{K/k}(\theta)$ where k runs through the three quadratic subfields of K, show that the algebraic integers θ in K have the form $\frac{1}{2}(\alpha + \beta\sqrt{2})$, where $\alpha = a + ib$ and $\beta = c + id$ are Gaussian integers. By considering $N_{K/k}(\theta)$ where $k = \mathbb{Q}(i)$ show that

$$\begin{aligned} a^2 - b^2 - 2c^2 + 2d^2 &\equiv 0 \pmod 4, \\ ab - 2cd &\equiv 0 \pmod 2. \end{aligned}$$

    Hence prove that an integral basis for K is $1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}$, and calculate the discriminant D_K.

11. Suppose that K is a number field of degree $n = r + 2s$ in the usual notation (r is the number of real embeddings of K and s the number of pairs of complex conjugate embeddings). Show that the sign of the discriminant D_K is $(-1)^s$.

12. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree n, and $\theta \in \mathbb{C}$ a root of f.

    (i) Show that $\mathrm{disc}(f) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(f'(\theta))$ where $K = \mathbb{Q}(\theta)$.

    (ii) Let $f(X) = X^n + aX + b$. Write down the matrix representing multiplication by $f'(\theta)$ with respect to the basis $1, \theta, \ldots, \theta^{n-1}$ for K. Hence show that

$$\mathrm{disc}(f) = (-1)^{\binom{n}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).$$

The following extra questions are just for fun. They can be answered using material from the Part IB course *Groups Rings and Modules*.

12. Let $\omega \neq 1$ be a cube root of unity, and let $p \neq 3$ be a prime.

    (i) By considering units in $\mathbb{Z}[\omega]$ show that $x^2 + 3y^2$ represents p if and only if $x^2 + xy + y^2$ represents p.

    (ii) Use that $\mathbb{F}_p^*$ is cyclic to find a condition on p for the congruence $x^2 + x + 1 \equiv 0 \pmod p$ to be soluble.

    (iii) Use unique factorisation in $\mathbb{Z}[\omega]$ to determine the set of primes in (i).

13. Show that the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean. Hence find all integer solutions to the equations $y^2 = x^3 - 4$ and $y^2 + y = x^3 - 2$.

14. Let $n \geq 3$ be an integer. Suppose $f, g, h \in \mathbb{C}[X]$ are coprime polynomials satisfying $f^n + g^n = h^n$. Use unique factorisation in $\mathbb{C}[X]$ to construct a new solution to this equation involving polynomials of smaller degree. Deduce that f, g, h must be constant.

Lent Term 2016

Number Fields: Example Sheet 2 of 3

1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathcal{O}_K$. Determine the factorisations into prime ideals of $\mathfrak{a}+\mathfrak{b}$ and $\mathfrak{a}\cap\mathfrak{b}$ in terms of those for $\mathfrak{a}$ and $\mathfrak{b}$. Show that if $\mathfrak{a}+\mathfrak{b}=\mathcal{O}_K$ then $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$ and there is an isomorphism of rings $\mathcal{O}_K/\mathfrak{ab}\cong\mathcal{O}_K/\mathfrak{a}\times\mathcal{O}_K/\mathfrak{b}$.

2. Let $K=\mathbb{Q}(\sqrt{-5})$. Show by computing norms, or otherwise, that $\mathfrak{p}=(2,1+\sqrt{-5})$, $\mathfrak{q}_1=(7,3+\sqrt{-5})$ and $\mathfrak{q}_2=(7,3-\sqrt{-5})$ are prime ideals in $\mathcal{O}_K$. Which (if any) of the ideals $\mathfrak{p},\mathfrak{q}_1,\mathfrak{q}_2,\mathfrak{p}^2,\mathfrak{pq}_1,\mathfrak{pq}_2$ and $\mathfrak{q}_1\mathfrak{q}_2$ are principal? Factor the principal ideal $(9+11\sqrt{-5})$ as a product of prime ideals.

3. Let $\mathfrak{a}\subset\mathcal{O}_K$ be a non-zero ideal, and m the least positive integer in $\mathfrak{a}$. Prove that m and $N\mathfrak{a}$ have the same prime factors.

4. Let $K=\mathbb{Q}(\sqrt{35})$ and $\omega=5+\sqrt{35}$. Verify the ideal equations $(2)=(2,\omega)^2$, $(5)=(5,\omega)^2$ and $(\omega)=(2,\omega)(5,\omega)$. Show that the class group of K contains an element of order 2. Find all ideals of norm dividing 100 and determine which are principal.

5. Let p be an odd prime and $K=\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive pth root of unity. Determine $[K:\mathbb{Q}]$. Calculate $N_{K/\mathbb{Q}}(\pi)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\pi)$ where $\pi=1-\zeta_p$.

   (i) By considering traces $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^j\alpha)$ show that $\mathbb{Z}[\zeta_p]\subset\mathcal{O}_K\subset\frac{1}{p}\mathbb{Z}[\zeta_p]$.

   (ii) Show that $(1-\zeta_p^r)/(1-\zeta_p^s)$ is a unit for all $r,s\in\mathbb{Z}$ coprime to p, and that $\pi^{p-1}=up$ where u is a unit.

   (iii) Prove that the natural map $\mathbb{Z}\to\mathcal{O}_K/(\pi)$ is surjective. Deduce that for any $\alpha\in\mathcal{O}_K$ and $m\geq 1$ there exist $a_0,\ldots,a_{m-1}\in\mathbb{Z}$ such that

$$\alpha\equiv a_0+a_1\pi+\ldots+a_{m-1}\pi^{m-1}\pmod{\pi^m\mathcal{O}_K}.$$

   (iv) Deduce that $\mathcal{O}_K=\mathbb{Z}[\zeta_p]$.

6. Let $K=\mathbb{Q}(\sqrt{-d})$ where d is a positive square-free integer. Establish the following facts about the factorisation of principal ideals in $\mathcal{O}_K$.

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

   (ii) If $d\equiv 1$ or $2\pmod 4$ then $(2)=\mathfrak{p}^2$ where $\mathfrak{p}$ is not principal unless $d=1$ or 2.

   (iii) If $d\equiv 7\pmod 8$ then $(2)=\mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}$ is not principal unless $d=7$.

   Deduce that if K has class number 1 then either $d=1$, 2 or 7, or d is prime and $d\equiv 3\pmod 8$.

7. Let $K=\mathbb{Q}(\sqrt{-m})$ where $m>0$ is the product of distinct primes $p_1,\ldots,p_k$. Show that $(p_i)=\mathfrak{p}_i^2$ where $\mathfrak{p}_i=(p_i,\sqrt{-m})$. Show that just two of the ideals $\prod\mathfrak{p}_i^{r_i}$ with $r_i\in\{0,1\}$ are principal. Deduce that the class group Cl_K contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$. [*If you like, just do the case* $m\not\equiv 3\pmod 4$.]

8. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 4X + 7$. Determine the ring of integers and discriminant of K. Determine the factorisation into prime ideals of $p\mathcal{O}_K$ for $p = 2, 3, 5, 7, 11$. Find all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $N\mathfrak{a} \leq 11$.

9. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 + X^2 - 2X + 8$. [*This polynomial is irreducible over* $\mathbb{Q}$ *and has discriminant* -4×503.]

   (i) Show that $\beta = 4/\alpha \in \mathcal{O}_K$ and $\beta \notin \mathbb{Z}[\alpha]$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

   (ii) Show that there is an isomorphism of rings $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Deduce that 2 splits completely in K.

   (iii) Use Dedekind's criterion to show that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any θ.

10. (i) Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. Show that every ideal in the ring $\mathcal{O}_K/\mathfrak{a}$ is principal. [*Hint: Use Question 1 to reduce to the case* $\mathfrak{a}$ *is a prime power.*]

    (ii) Deduce that every ideal in $\mathcal{O}_K$ can be generated by 2 elements.

11. Show that $\mathbb{Q}(\sqrt{-d})$ has class number 1 for $d = 1$, 2, 3, 7, 11, 19, 43, 67, 163.

And some extra questions, just for fun.

12. For $\mathfrak{a}$ an ideal in $\mathcal{O}_K$ let $\phi(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})^*|$. Show that $\phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} (1 - \frac{1}{N\mathfrak{p}})$.

13. Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f(x))$, where $f(x)$ is the minimum polynomial of α. The trace form on K defines a bilinear form on the real vector space $\mathbb{R}[x]/(f(x))$. Show that the signature of this form is $(r + s, s)$, where $r + 2s = n$, r is the number of embeddings of K into $\mathbb{R}$.

14. Prove Stickelberger's criterion, that $D_K \equiv 0, 1 \pmod 4$. [*Hint: Start by writing* $D_K = (P - N)^2 = (P + N)^2 - 4PN$ *where* P *is a sum over even permutations and* N *is a sum over odd permutations. Then show that* $P + N, PN \in \mathbb{Z}$.]
    Hence compute the ring of integers of $\mathbb{Q}[X]/(f(X))$ where $f(X) = X^3 - X + 2$.

15. Let $B_{r,s}(t) = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum |y_i| + 2\sum |z_j| \leq t\}$. Show that $volB_{r+1,s}(t) = \int_{-t}^{t} volB_{r,s}(t - |y|)dy$, and $volB_{r,s+1}(t) = \int\int_{|z| \leq t/2} volB_{r,s}(t - 2|z|)$.

    Hence show by induction that $volB_{r,s}(t) = 2^r(\frac{\pi}{2})^s \frac{t^n}{n!}$. [You should do the second integral by choosing polar coordinates, $z = re^{i\theta}$.]

Lent Term 2016

Number Fields: Example Sheet 3 of 3

1. Let $K = \mathbb{Q}(\sqrt{26})$ and let $\varepsilon = 5 + \sqrt{26}$. Use Dedekind's theorem to show that the ideal equations

$$(2) = (2, \varepsilon + 1)^2, \quad (5) = (5, \varepsilon + 1)(5, \varepsilon - 1), \quad (\varepsilon + 1) = (2, \varepsilon + 1)(5, \varepsilon + 1)$$

hold in K. Using Minkowski's bound, show that K has class number 2. Verify that ε is the fundamental unit. Deduce that all solutions in integers x, y to the equation $x^2 - 26y^2 = \pm 10$ are given by $x + \sqrt{26}y = \pm\varepsilon^n(\varepsilon \pm 1)$ for $n \in \mathbb{Z}$.

2. Find the factorisations into prime ideals of (2) and (3) in $K = \mathbb{Q}(\sqrt{-23})$. Verify that $(\omega) = (2, \omega)(3, \omega)$ where $\omega = \frac{1}{2}(1 + \sqrt{-23})$. Prove that K has class number 3.

3. Find the factorisations into prime ideals of (2), (3) and (5) in $K = \mathbb{Q}(\sqrt{-71})$. Verify that

$$(\alpha) = (2, \alpha)(3, \alpha)^2 \quad \text{and} \quad (\alpha + 2) = (2, \alpha)^3(3, \alpha - 1)$$

where $\alpha = \frac{1}{2}(1 + \sqrt{-71})$. Find an element of $\mathcal{O}_K$ with norm $2^a \cdot 3^b \cdot 5$ for some $a, b \geq 0$. Hence prove that the class group of K is cyclic and find its order.

4. Compute the ideal class group of $\mathbb{Q}(\sqrt{d})$ for $d = -30$, -13, -10, 19 and 65.

5. (i) Find the fundamental unit in $\mathbb{Q}(\sqrt{3})$. Determine all the integer solutions of the equations $x^2 - 3y^2 = m$ for $m = -1, 13$ and 121.

   (ii) Find the fundamental unit in $\mathbb{Q}(\sqrt{10})$. Determine all the integer solutions of the equations $x^2 - 10y^2 = m$ for $m = -1, 6$ and 7.

6. Find all integer solutions of the equations $y^2 = x^3 - 13$ and $y^2 = x^5 - 10$.

7. Let $K = \mathbb{Q}(\sqrt{-d})$ where $d > 3$ is a square-free integer.

   (i) Show that if $\mathcal{O}_K$ is Euclidean then it contains a principal ideal of norm 2 or 3. [*Hint: Suppose that* $\phi : \mathcal{O}_K - \{0\} \to \mathbb{N}$ *is a Euclidean function. Then choose* $x \in \mathcal{O}_K - \{0, \pm 1\}$ *with* $\phi(x)$ *minimal.*]

   (ii) Use your answer to Problem Sheet 2, question 11 to give an example where $\mathcal{O}_K$ is a PID, but is not Euclidean.

8. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Describe the ring $\mathcal{O}_K/2\mathcal{O}_K$ as explicitly as you can. [*The answer depends on d mod* 8.] Show that $\mathbb{Z}[\sqrt{d}]^\times \subset \mathcal{O}_K^\times$ has index 1 or 3. Give an example where the index is 3.

9. Let p be an odd prime.

   (i) Compute the discriminant of $(X^p - 1)/(X - 1)$. Deduce that $\mathbb{Q}(\zeta_p)$ contains a quadratic field with discriminant $\pm p$.

   (ii) Show using the Minkowski bound that $\mathbb{Z}[\zeta_p]$ is a UFD for $p = 5$ and $p = 7$.

10. Let $K = \mathbb{Q}(\zeta_8)$ and $\mathfrak{p} = (1 - \zeta_8)$. Show that $N\mathfrak{p} = 2$ and that complex conjugation acts trivially on $\mathcal{O}_K/\mathfrak{p}^2$. Find a fundamental unit in K. [*Hint: First find a fundamental unit in* $\mathbb{Q}(\zeta_8) \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$. *Then imitate a proof in lectures.*]

11. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 3X + 1$.

    (i) Show that f is irreducible over $\mathbb{Q}$ and compute its discriminant.

    (ii) Show that $3\mathcal{O}_K = \mathfrak{p}^3$ where $\mathfrak{p} = (\alpha + 1)$ is a prime ideal in $\mathcal{O}_K$ with residue field $\mathbb{F}_3$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$. [*Hint: See Sheet 2, Question 5.*]

    (iii) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Compute the class group of K.

The following extra questions are just for fun. Questions 18 and 19 need Galois Theory.

13. Let K be a number field. Show that there is a number field L containing K such that for every ideal $\mathfrak{a} \subset \mathcal{O}_K$ the ideal in $\mathcal{O}_L$ generated by $\mathfrak{a}$ (denoted $\mathfrak{a}\mathcal{O}_L$) is principal. [*Hint: Use that some power of* $\mathfrak{a}$ *is principal.*]

14. Let L/K be an extension of number fields.

    (i) Show that if $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$ then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ and $N\mathfrak{P}$ is a power of $N\mathfrak{p}$.

    (ii) Let $L = \mathbb{Q}(i, \sqrt{5})$. Show that $|D_L| \leq 400$ and that the primes 2 and 3 are inert in some quadratic field $K \subset L$. Deduce that L has class number 1.

15. Show that there are no integer solutions to $x^2 - 82y^2 = \pm 2$.

16. Let L/K be an extension of number fields. Show that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ then $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. [*Hint: Let* $x_1, \ldots, x_m$ *generate* $\mathcal{O}_L$ *as an* $\mathcal{O}_K$*-module. If* $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ *then we can write* $x_i = \sum a_{ij}x_j$ *for some* $a_{ij} \in \mathfrak{p}$.] Deduce that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$ with $\mathfrak{a}\mathcal{O}_L = \mathfrak{b}\mathcal{O}_L$ then $\mathfrak{a} = \mathfrak{b}$.

17. Let L/K be an extension of number fields. Let p be a rational prime. Show using Questions 14(i) and 16 that (i) If p is unramified in L then it is unramified in K. (ii) If p is totally ramified in L then it is totally ramified in K.

18. Let K be a number field with $K/\mathbb{Q}$ Galois. Let p be a rational prime with $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals. Use the Chinese Remainder Theorem (Sheet 2, Question 1) to find $x \in \mathfrak{p}_1$ with $x \notin \mathfrak{p}_i$ for $2 \leq i \leq r$. By considering $N_{K/\mathbb{Q}}(x)$ show that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

19. Let $K = \mathbb{Q}(\sqrt{-23}) \subset L = \mathbb{Q}(\zeta_{23})$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime dividing 2. Show that if $\mathfrak{p}\mathcal{O}_L = x\mathcal{O}_L$ for some $x \in \mathcal{O}_L$ then $\mathfrak{p}^{11}\mathcal{O}_L = N_{L/K}(x)\mathcal{O}_L$. Deduce by Questions 2 and 16 that $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

20. Let $d \neq 0, 1$ be a square free integer, $K = \mathbb{Q}(\sqrt{d})$, $D = D_K$. Define $\chi_D(p) = \left(\frac{D}{p}\right)$ if $p > 2$, and p prime, and $\chi_D(2) = 1$ if $d = 1 \bmod 8$, $\chi_D(2) = -1$ if $d = 5 \bmod 8$, and $\chi_D(2) = 0$ otherwise. Extend this to a function on $\mathbb{Z}$ by setting $\chi_D(mn) = \chi_D(m)\chi_D(n)$. Using quadratic reciprocity, show that χ_D is D-periodic: $\chi_D(a + Db) = \chi_D(a)$, $a, b \in \mathbb{Z}$. [*Hint: You will find it easier to do the cases* $d = 3, 2, 1 \bmod 4$ *separately*].