PartII Number Fields

zc231

Each question will be labeled in the form $\alpha, \beta\gamma$ where $\alpha \in \{1, 2, 3, 4\}$ represents the paper number, $\beta\gamma$ represents the question number in that paper. For example, 1,11G means question 11G in paper 1. I will omit the proofs in the notes or book work. The solutions provided might not be the best ways to solve the problems and if you find any mistakes or if you have any elegant ways of solving some of the problems please email me at zc231@cam.ac.uk.

2009

1,20H (i) book work (use structure theorem of finitely generated module over PID). (ii) Discriminant is $-4(2^3) - 27 = -59$ which is square free so $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where α is a root of $X^3 + 2X + 1$. (iii) as d is square free so f, g are both irreducible and hence $\mathbb{Z}[X]/(f), \mathbb{Z}[X]/(g)$ are fields of degree 2 and by completing the squares they are both isomorphic to $\mathbb{Z}[X]/(x^2 - d)$.

2,20H (i) book work. (ii) Minkowski bound is 5. So we consider prime ideal with norm $2, 3, 5$. 2 ramifies as it divides the discriminant say $\langle 2\rangle = I_2^2$. Similarly $\langle 3\rangle = I_3^2$. 5 splits into product of two distinct ideals say $\langle 5\rangle = I_5 J_5$. Now we consider $3 + \sqrt{-21}$ which has norm 30 and hence we must have

$$\langle 3 + \sqrt{-21}\rangle = I_2 I_3 I_5 \text{ or } \langle 3 + \sqrt{-21}\rangle = I_2 I_3 J_5.$$

This shows that $I_2 I_3 = I_5$ or J_5 in the class group. Finally $I_2 \neq I_3$ in the class group as the product of them is not principal (no element of norm 6). Therefore we assume $I_2 I_3 = I_5$ in the class group and so $I_2 I_3 = J_5$ so the class group is isomorphic to $C_2 \times C_2$, generated by I_2, I_3.

Thus the class number is prime to 3 so for the last part we conclude

$$y + \sqrt{-21} = (a + b\sqrt{-21})^3$$

and so by comparing coefficients,

$$y = a^3 - 63ab^2, 1 = (3a^2 - 21b^2)b$$

and since $3 \nmid 1$ so there is no solution.

4,20H The first part is book work (use the logarithm map to identify the units as a lattice with rank at most $r + s - 1$). If u is a unit and is torsion then u must be a root of unity and hence the torsion group is μ_n for some n. The only roots of unity in $\mathbb{Q}(\sqrt{11})$ is ± 1 and we have $r + s - 1 = 1$ so we have one generator. Use continue fraction algorithm to find a solution greater than 1 for

$$x^2 - 11y^2 = 1$$

with the smallest modulus (which is the generator). We take $10 + 3\sqrt{11}$ and so the units are

$$\{\pm(10 + 3\sqrt{11})^n : n \in \mathbb{Z}\}.$$

2010

1,20G As m is even so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-m}]$. As the class number is prime to 3, therefore we conclude that

$$y + \sqrt{-m} = (a + b\sqrt{-m})^3$$

and so by comparing the coefficients of $\sqrt{-m}$ we have

$$1 = (3a^2 - b^2 m)b$$

and so $b = \pm 1$. So we have $3a^2 - m = 1$ or $3a^2 - m = -1$ and at most one of these have solutions because we require $1 + m$ or $-1 + m$ to be a multiple of 3. Thus at most one of these holds and so we have at most one solution for b and then two solutions for a.

2,20G Minkowski bound is 4 and so we consider $p = 2, 3$. 2 ramifies as $2\big|14$ so let $\langle 2\rangle = I_2^2$ and by Dedekind criteria 3 splits say $\langle 3\rangle = I_3 J_3$. Now consider the element $2 + \sqrt{-14}$ which has norm $18 = 2 \cdot 3^2$ and as it is not real so we must have

$$\langle 2 + \sqrt{-14}\rangle = I_2 I_3^2 \text{ or } \langle 2 + \sqrt{-14}\rangle = I_2 J_3^2$$

so either $I_2 I_3^2 = 1$ or $I_2 J_3^2 = 1$ in the class group. But in either case we have $I_3^2 = I_2 = J_3^2$ so we conclude the class group is C_4 generated by I_3 (note I_3 is not principal as we have no element of norm 3).

4,20G Reduce $x^3 - x + 3$ mod 2 and this is not irreducible over $\mathbb{F}_2[x]$ hence it is irreducible over $\mathbb{Z}[x]$ so $[K : \mathbb{Q}] = 3$. The discriminant is $4 - 27 \cdot 3^2 = -239$ which is square free and so $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

2011

1,20F Minkowski bound is 5 so we consider $p = 2, 3, 5$. 2 ramifies as it divides the discriminant so $\langle 2\rangle = I_2^2$. As $-17 \equiv 3 \bmod 4$ so by Dedekind criteria we have

$$\langle 3\rangle = I_3 J_3, \langle 5\rangle = I_5$$

where I_5 has norm 25. Clearly as no element has norm 2 or 3 so I_2, I_3, J_3 are not principal. Further consider the element $1 + \sqrt{-17}$ which has norm 18 and so we must have

$$\langle 1 + \sqrt{-17}\rangle = I_2 I_3^2 \text{ or } \langle 1 + \sqrt{-17}\rangle = I_2 J_3^2.$$

In both cases we have $I_2 = I_3^2 = J_3^2$ so the class group is C_4, generated by I_3.

As the class number is prime to 5, so we must have

$$y + \sqrt{-17} = (a + b\sqrt{-17})^5$$

and so by comparing coefficients of $\sqrt{-17}$ we have

$$1 = 5a^4 b - 170a^2 b^3 + 289b^5.$$

Then $b = \pm 1$ and since $17 \big| 170, 289$ so $17 \big| 5a^4 b$ and so $17 \big| a$. Thus, $17^3 \big| 5a^4 b - 170a^2 b^3$ and so $17^3 \big| 289b^5$ which is impossible. Therefore we have no solution.

2,20F (i) is book work (by considering the discriminant $4d$ and so the index is either 1 or 2). (ii) it is clear that if $\alpha = 2^{\frac{1}{3}}$ and $\beta = 4^{\frac{1}{3}}$ then $\beta = \alpha^2$ and $\beta^2 = 2\alpha$ and so these two fields are the same. It is clear that α is an algebraic integer and we claim $\alpha \notin \mathbb{Z}[\beta]$. Suppose

$$\alpha = a + b\beta + c\beta^2$$

then $\beta = \alpha^2$ and $\beta^2 = 2\alpha$ then we have a polynomial of α which is

$$b\alpha^2 + \alpha(2c - 1) + a = 0$$

and as the minimal polynomial of α has degree 3 so we must have $2c - 1 = 0$ which gives $c = \frac{1}{2}$ not an integer.

4,20F Consider the logarithm map $\alpha \mapsto (\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|)$ where σ_1, σ_2 are the two real embeddings and the image is a subset of $\mathbb{R}^2$. The units are the subset in the image with $x_1 + x_2 = 0$ which is a lattice of rank 1, say H Now let

$$S_t = \{(x_1, x_2) : |x_1| + |x_2| \leq t\}$$

and S_t is convex, symmetric and compact and the volume of S_t is $2t^2$. As the covolume of H is fixed so we pick t large enough so that $S_t = 4cov(H)$ then by convex body theorem we have $x \neq 0$, $x \in S_t \cap H$. Then $x = (\sigma_1(y), \sigma_2(y))$ for some $y \in \mathcal{O}_K$ and $x \neq 0$ so y is not ± 1. Finally $x \in H$ so y is a unit.

For the last part, we show that $8 + 3\sqrt{7}$ is the smallest unit greater than 1 (which then shows it is a generator). Any unit must have the form $a + b\sqrt{7}$ and if $a + b\sqrt{7}$ is a unit, so is $a - b\sqrt{7}$ and if one of them is bigger than one then other one must be less than 1 so we may assume $b > 0$. We check there is no unit with $b = 1$ or 2 and for $b = 4, 5, 6$ we have no unit so the next one must take $b \geq 7$ and $4\sqrt{7} > 8$ therefore we conclude $8 + 3\sqrt{7}$ is the smallest unit bigger than 1.

2012

4,20F The first part is clear by computing the relative traces and use the fact when $p, q \equiv 3 \bmod 4$ we have $\mathcal{O}_{\mathbb{Q}[\sqrt{p}]} = \mathbb{Z}[\sqrt{p}]$,$\mathcal{O}_{\mathbb{Q}[\sqrt{q}]} = \mathbb{Z}[\sqrt{q}]$. Then compute the relative norm by taking $k = \mathbb{Q}[\sqrt{q}]$ we have

$$\frac{1}{4}(a^2 + c^2 - b^2p - d^2pq) + \frac{1}{2}(ac - bdp) \in \mathbb{Z}[\sqrt{q}]$$

and so we require

$$a^2 + c^2q - b^2p - d^2pq \equiv 0 \bmod 4, ac - bdq \equiv 0 \bmod 2.$$

Thus if c, d are both even we have $4 \big| a^2 - b^2p$ and since $p \equiv 3 \bmod 4$ so we have $a^2 - 3b^2 \equiv 0 \bmod 4$ and so as $a^2 \equiv 0, 1 \bmod 4$ so we must have $a^2, b^2 \equiv 0 \bmod 4$ so a, b are both even. Further if c is odd d is even then we must have a even b odd. If c is even and d is odd then we must have a odd b even. Then we check indeed that $\frac{\sqrt{p}+\sqrt{q}}{2}, \frac{1+\sqrt{pq}}{2}$ are algebraic integers. Finally if c, d are both odd then a, b must be both odd so we have considered all possibilities and so we have the required integral basis.

2,20F Discriminant of f is -47 which is square free so we can apply Dedekind criteria. Then we have

$$\langle 2 \rangle = I_2 J_2, \langle 3 \rangle = I_3 J_3$$

and by Dedekind criteria we let I_2 be the ideal containing α and I_3 be the ideal containing α. The norm of α is 12 and so $\langle \alpha \rangle = I_2^2 I_3$. The norm of $\alpha + 2$ is 18 and $\alpha + 2$ is contained in I_2 and J_3 and so $\langle \alpha + 2 \rangle = I_2 J_3^2$. Thus we have $J_3^4 = I_3$ in the class group and since $J_3 I_3 = 1$ in the class group so we have $J_3^5 = 1$ and we see then I_2, J_2, I_3 can be generated by J_5 so the class group is C_5.

Then for the last part we can replace y by $-y$ so we consider the solution to

$$y^2 - y + 12 = 3x^5$$

and so

$$\langle y - \alpha \rangle \langle y - \bar{\alpha} \rangle = \langle 3 \rangle \langle x \rangle^5.$$

Since $\langle 3 \rangle = I_3 J_3$ which are conjugates so we may assume $I_3 \big| \langle y - \alpha \rangle$ (as $y - \alpha, y - \bar{\alpha}$ are conjugates). Thus we conclude that

$$\langle y - \alpha \rangle = I_3 I^5$$

for some I but I^5 is principal and hence this shows I_3 is principal which is a contradiction.

1,20F Norm of unit is ± 1. Clearly if K is imaginary field then this is clear because the only units of norm ± 1 are ± 1 (and ζ_3 in the case $d = -3$). Now suppose K is real and then the only roots of unity are ± 1. Suppose K has no non-trivial unit then $K/\{\pm 1\}$ is trivial. Suppose K has a non-trivial unit then by using real embeddings we take the smallest one with modulus greater than 1 say u. Then for any unit v greater than 1 pick the least n such that $u^n > v$ then $u^{-n}v > 1$ and by definition of n we have

$$u^n v^{-1} > 1, u^n v^{-1} \leq u$$

and so by definition of u we have $u^n v^{-1} = u$. Therefore every unit greater than 1 is generated by u and every unit between 0 and 1 is an inverse of some unit bigger than 1. Thus we conclude that the set of units is $\{\pm 1 u^n : n \in \mathbb{Z}\}$ and hence the quotient is cyclic.

For $\mathbb{Q}(\sqrt{-3})$ we have $U = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. For $\mathbb{Q}(\sqrt{11})$ the fundamental unit is $10 + 3\sqrt{11}$.

For $n = -1$, we reduce both sides modulo 11 then we need $x^2 \equiv -1 \bmod 11$ which is not soluble. For $n = 5$ we take a solution $4 + \sqrt{11}$ and so the solutions are $\pm(8 + 3\sqrt{11})^n(4 + \sqrt{11})$. For $n = 14$ we have $\pm(8 + 3\sqrt{11})^n(5 + \sqrt{11})$.

2013

4,20H The minimal polynomial of $\frac{1+\sqrt{65}}{2}$ is $x^2 - x - 16$. Thus we have

$$\langle 2\rangle = I_2 J_2, \langle 3\rangle = I_3, \langle 5\rangle = I_5^2.$$

Consider the element $2 - \alpha$ where α is a root of $x^2 - x - 16 = 0$ and the norm of this element is 10 and hence

$$I_2 I_5 = \langle 2 - \alpha\rangle \text{ or } J_2 I_5 = \langle 2 - \alpha\rangle$$

but in either case as I_5^2 is principal so we have $I_2 = J_2 = I_5$ in the class group. Therefore the ideals of norm 10 are principal and so the class group is C_2.

2,20H For (ii) the condition shows that the absolute value of the norm of α is at most 1 and since the norm is integer so $N(\alpha) = \pm 1$ or 0 and so $\alpha = 0$ or unit. Further if $\alpha \neq 0$ then equality must hold, i.e. every conjugate of α has absolute value 1 so we consider the intersection of $\mathcal{O}_K$ with the unit circle

$$C = \{(x_1, \ldots, x_n) : |x_i| = 1 \forall i\}$$

and since C is compact and $\mathcal{O}_K$ is a lattice so the intersection is finite and hence α must be a root of unity.

We have $[K : \mathbb{Q}] = 4$ and so $[K : k] = 2$. Since k is real so the Galois group of K/k is generated by a lift of complex conjugate so we have

$$N_{K/k}(1 + \zeta) = (1 + \zeta)(1 + \zeta^{-1}) = 2 + \sqrt{3}.$$

The rank of units in K is 1 (as $2s = 4$) which is the same as the rank of units in k. Since k is a subfield of K we conclude that if we pick a generator u in K then there exists n with u^n being a generator in k. As u^n is real so we conclude $u = vw$ where v is real and w is a root of unity. As the only roots of unity in K are μ_{12} so we can multiply u by suitable root of unity and so we can assume u is real. Therefore $u \in K \cap \mathbb{R} = k$ and so $n = \pm 1$. This gives the required result. Then the fundamental units of k and K can be chosen to be the same so we take $u = 2 + \sqrt{3}$.

1,20H (i) is clear as if $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = r$ then $r^2 \mathcal{D}_K = \text{disc}(f)$. The minimal polynomial of β is $x^3 - x + 1$. The discriminant of $x^3 - x + 1$ is -23 which is square free and so $\mathcal{D}_K = -23$. Then we compute the discriminant of $\mathbb{Z}[\alpha]$ which is -16767 and $\frac{-16767}{-23} = 729 = 27^2$ so the index is 27. In case you have trouble to find the minimal polynomial of β, we have $\alpha = 1 - \frac{3}{\beta}$ and substitute this into $f(x)$ gives a cubic polynomial in terms of β.