MAT415: MIDTERM SOLUTIONS

Each question is worth 12 points, with each part being worth an equal number of points.

(1) Let $K = \mathbb{Q}[x]/(x^4 + x^3 + x^2 + x + 1)$, so that x is a primitive 5'th root of unity.

(a) Using Discriminants (or otherwise), prove that $\mathcal{O}_K = \mathbb{Z}[x]$.

Proof. We consider the Discriminant of $\mathbb{Z}[x]$. As a basis, we take $1, x, x^2, x^4$. The Discriminant of $\mathbb{Z}[x]$ is thus the square of the absolute value of $\begin{pmatrix} 1 & 1 & 1 & 1 \\ x & x^2 & x^3 & x^4 \\ x^2 & x^4 & x & x^3 \\ x^3 & x & x^4 & x^2 \end{pmatrix}$ This is a vandermonde determinant, and thus

$$\begin{aligned} \mathrm{Disc}_{\mathbb{Z}[x]} &= |(1-x)(1-x^2)(1-x^4)(x-x^2)(x-x^4)(x^2-x^4)|^2 \\ &= |(1-x)^2(1-x^2)^2(1-x^3)(1-x^4)|^2 \end{aligned}$$

Note that $(z-x)(z-x^2)(z-x^3)(z-x^4) = z^4+z^3+z^2+z+1$, so plugging in $z = 1$ into the previous equation we get

$$\mathrm{Disc}_{\mathbb{Z}[x]} = 25|(1-x)(1-x^2)|^2$$

Now,

$$|(1-x)^2(1-x^2)^2| = |(1-x)(1-x^2)(x^4-1)(x^3-1)| = 5.$$

Thus we conclude that $\mathrm{Disc}_{\mathbb{Z}[x]} = 125$. Alternatively, to calculate the discriminant one can use the trace pairing. Note that the trace of 1 is 4 and the trace of x, x^2, x^3 is $x+x^2+x^3+x^4 = -4$ since x, x^2, x^3, x^4 are Galois conjugates. So the Discrminant is the same as the absolute value of the determinant of $\begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 4 \\ -1 & -1 & 4 & -1 \end{pmatrix}$ which can be evaluated to 125.

Now, the Minkowski bound says that

$$|\mathrm{Disc}_K|^{\frac{1}{2}}| \geq \frac{4^4}{4!}(\pi/4)^2 = \frac{2\pi^2}{3} \geq 6$$

and thus $|\mathrm{Disc}_K| \geq 36$. However, $\mathrm{Disc}_{\mathbb{Z}[x]}$ is an integer square times Disc_K, and so $\mathrm{Disc}_K = 125$.

□

(b) For each prime p, depending on what p is modulo 5 figure out how many prime ideals P in $\mathcal{O}_K$ satisfy $P \cap \mathbb{Z} = (p)$.

Proof. We are interested in the number of maximal ideals containing $p\mathcal{O}_K$, which is equivalent to the number of maximal ideals in

$$\mathcal{O}_K/(p) = \mathbb{Z}[x]/(p, 1+x+x^2+x^3+x^4) = \mathbb{F}_p[x]/(1+x+x^2+x^3+x^4).$$

Now, if $p = 5$ then $1+x+x^2+x^3+x^4 = (1-x)^4$, so there is only one prime ideal (which is totally ramified).

If $p \neq 5$, then $\overline{\mathbb{F}_p}$ contains 5 roots of unity (and thus 4 primitive roots of unity). Now since the multiplicative group of a finite field is cyclic, $\mathbb{F}_{p^n}^\times$ contains a 5-torsion element iff $5|p^n - 1$.

If $p \equiv 1 \mod 5$ then $\mathbb{F}_p$ contains all the roots of unity. And thus $1+x+x^2+x^3+x^4$ factors into 4 linear factors, and so there are 4 prime ideals.

If $p \equiv 4 \mod 5$ then $\mathbb{F}_{p^2}$ contains the 5'th roots of unity but $\mathbb{F}_p$ does not. Thus the roots come in Galois conjugate pairs, and so $1+x+x^2+x^3+x^4$ factors into 2 quadratics, and so there are two prime ideals.

If $p \equiv 2, 3 \mod 5$, then $\mathbb{F}_{p^4}$ contains the 5'th roots of unity but $\mathbb{F}_{p^2}$ does not. Thus the roots generate $\mathbb{F}_{p^4}$ and are all Galois conjugate. So $1+x+x^2+x^3+x^4$ is irreducible and so there $p\mathcal{O}_K$ is a prime ideal.

□

(2) (a) Determine the class group of $K = \mathbb{Q}(\sqrt{-22})$.

Proof. Sinze $-22 \equiv 2 \mod 4$ and so the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-22}]$. The Discriminant is -88, and so the Minkowski bound is

$$\sqrt{88} \cdot \frac{2!}{2^2} \cdot \frac{4}{\pi} = \sqrt{176}/\pi < 14/3 < 5.$$

Thus the class group is generated by the prime ideals above 2 and 3.

Now $(2) = (2, \sqrt{-22})^2$ while 3 remains prime since -22 is not a square modulo 3. Thus $(2, \sqrt{-22})$ generates the class group and is of order at most 2. So to prove that the class group is $\mathbb{Z}/2\mathbb{Z}$ it suffices to prove that $(2, \sqrt{-22})$ is not principal. But if

it were, there would be an element $x + y\sqrt{-22}$ of norm 2, and thus a solution to $x^2 + 22y^2 = 2$, which there evidently is not.

□

(b) Find all integer solutions to $x^3 = y^2 + 550$. **Hint: Think in terms of ideals**

Proof. Write $x^3 = y^2 + 550 = (y + 5\sqrt{-22})(y - 5\sqrt{-22})$. Now consider this as as equality of principle ideals in $\mathcal{O}_K$.
We first claim that $(y+5\sqrt{-22})$ and $(y-5\sqrt{-22})$ are relatively prime, or in other words that $I = (y+5\sqrt{-22}, y-5\sqrt{-22})$ is all of $\mathcal{O}_K$. Note that I contains $10\sqrt{-22}$ and hence 2200 and also $2y$ and x^3. Thus, if we prove that $2, 5, 11$ are relatively prime to x it will follows that I contains 1 and thus is equal to $\mathcal{O}_K$. Now if $2|x$ then $2|y$ and thus $4|x^3 - y^2 = 550$, which is false. Likewise we see that 11 does not divide x. If $5|x$, then $5|y$, so $x = 5m, y = 5n$ and $5m^3 = n^2 + 22$, and thus 3 is a quadratic residue mod 5 which is false. Hence, $(y + 5\sqrt{-22})$ is relatively prime to $(y - 5\sqrt{-22})$.
However, we know that there is unique factorization into prime ideals, and thus $(y + 5\sqrt{-22}) = J^3$ for some ideal J of $\mathcal{O}_K$. Moreover, J^3 is principal, and since the class group is $\mathbb{Z}/2\mathbb{Z}$ it follows that J^3 is principal, and thus we can write $J = (a + b\sqrt{-22})$ with $(a + b\sqrt{-22})^3 = \pm(y + 5\sqrt{-22})$, where we have used that the only units in $\mathcal{O}_K$ are ± 1.
Expanding and equating the coefficient of $\sqrt{-22}$ we see that $\pm 5 = -22b^3 + 3a^2b = b(3a^2 - 22)$. Hence $b = 1, -1, 5$ or -5. Checking the cases reveals that
$a = \pm 3, b = \pm 1$ are the only solutions. As $y = a^3 - 66ab^2$ this yields the solutions $(x, y) = (31, \pm 171)$.
Note: Another way to find x is to notice that its the norm of J, and thus $x = a^2 + 22b^2$.

□

(3) Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and set R to be the union of $\mathcal{O}_K$ over all number fields $K \subset \overline{\mathbb{Q}}$. Thus R is the set of all algebraic integers, and we showed in class that R is a ring.

(a) Does there exist a non-zero ideal I of R such that $I \cap \mathbb{Z} = \{0\}$?
Proof. No. Let $\alpha \in I$ be any non-zero element, and consider the product of all the distinct Galois conjugates of α. This is rational by Galois theory, non-zero since α is non-zero, and an algebraic integer. Hence its a non-zero integer. Moreover, its the product of α an an algebraic integer, hence its contained in I.

□

(b) Prove that every non-zero prime ideal of R is maximal.

Proof. Consider $P \subset R$ a non-zero prime ideal, and suppose for the sake of contradiction that M is a maximal ideal of R properly containing P. Let $x \in M \setminus P$, and let $K = \mathbb{Q}(x)$. Then K is an algebraic number field, so let $M_0 := \mathcal{O}_K \cap M$ and $P_0 := \mathcal{O}_K \cap P$. Now, M_0 and P_0 are prime ideals of $\mathcal{O}_K$ (the pullback of a prime ideal under any ring homomorphism is a prime ideal) and P_0 is non-zero since it contains a non-zero integer (as we established above). However, since prime ideals in $\mathcal{O}_K$ are either (0) or maximal, we have P_0 is maximal which is a contradiction since $x \in M_0 \setminus P_0$.

□

(c) Does there exists a prime ideal P of R such that R/P is a finite field?

Proof. No. Let $p\mathbb{Z} = P \cap \mathbb{Z}$, so that R/P is a field extension of $\mathbb{F}_p$. Let $f(x)$ be a monic irreducible polynomial of degree n over $\mathbb{F}_p$. Take $F(x)$ to be any monic lift of $f(x)$ to $\mathbb{Z}[x]$ of degree n. Then all roots of $F(x)$ are algebraic integers, and thus it has a root y in R. But then the reduction of y mod P is a root of $f(x)$, and thus R/P contains $\mathbb{F}_{p^n}$ for every n. Thus R/P contains $\overline{\mathbb{F}_p}$ and is infinite.**This in fact shows that $R/P \cong \overline{\mathbb{F}_p}$. Why?**

□

(d) Prove that R is not noetherian, but that every finitely-generated ideal of R is principal.

Proof. To see that R is not noetherian, let $\sqrt[2^n]{2}$ denote the unique real, positive 2^n'th root of 2. Let I_m be the ideal in R generated by $\sqrt[2^m]{2}$. We claim that $I_m \neq I_{m+1}$, which would prove R is not noetherian. Let $K_{m+1} := \mathbb{Q}[\sqrt[2^m]{2}]$. Then $I_m \cap \mathcal{O}_{K_{m+1}}$ is generated by $\sqrt[2^m]{2}$ and has norm 4 while $I_{m+1} \cap \mathcal{O}_{K_{m+1}}$ is generated by $\sqrt[2^{m+1}]{2}$ and has norm 2. Thus the ideals are distinct.

Finally, suppose that I is a finitely generated ideal of R. Let K be a number field containing a set of generators $(a_1, \ldots, a_n)$ for I. As we proved in class, there is some number field L in which $(I \cap K)\mathcal{O}_L$ becomes principal, say $\beta\mathcal{O}_L$. Thus I contains β, but also β generates each a_i over $\mathcal{O}_L$ and hence over R, and so I is equal to βR, as desired. □