MATH 6370: ASSIGNMENT #3

Due **April 26th**. Try as many of the following questions as you can. Solutions will be judged not only on correctness but also clarity and style of exposition. You can discuss/collaborate with other students in the class but you need to carefully indicate who contributed and how; solutions should be in your own words.

Problem 1:

(i) Compute the class group of $\mathbb{Q}(\sqrt{-47})$.

Set $K = \mathbb{Q}(\sqrt{-47})$. We have $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-47})/2]$ and $\mathcal{O}_K$ has discriminant -47. The Minkowski bound for K is

$$M_K = \sqrt{47} \cdot 4/\pi \cdot 2!/2^2 < 4.5.$$

Therefore, the group Cl_K is generated by primes $\mathfrak{p}$ of $\mathcal{O}_K$ with norm at most 4 (and hence divides 2, 3).

The minimal polynomial of $\theta := (1+\sqrt{-47})/2$ is $x^2 - x + 12$. Since $x^2 - x + 12 \equiv x(x-1) \pmod 2$, we deduce that

$$2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2',$$

where $\mathfrak{p}_2 = (2, \theta)$ and $\mathfrak{p}_2' = (2, \theta - 1)$. The primes $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ each have norm 2.

Lemma 1. *The class $[\mathfrak{p}_2]$ in Cl_K has order 5.*

Proof. Consider the element

$$\alpha := \frac{9+\sqrt{-47}}{2}$$

of $\mathcal{O}_K$. We have $N_{K/\mathbb{Q}}(\alpha) = (81+47)/4 = 128/4 = 32$. Therefore, the ideal $(\alpha) \subseteq \mathcal{O}_K$ has norm 32. Therefore, the only possible prime divisors of (α) are $\mathfrak{p}_2$ and $\mathfrak{p}_2'$.

If $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ both divide (α), then $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ divides (α); this is impossible since $\alpha/2 \notin \mathcal{O}_K$. Therefore, (α) is a power of $\mathfrak{p}_2$ or $\mathfrak{p}_2'$. We have $\alpha = 4 + \theta \in \mathfrak{p}_2$, so by comparing norms we deduce that

$$(\alpha) = \mathfrak{p}_2^5.$$

Therefore, $[\mathfrak{p}_2]^5 = 1$ in Cl_K. It remains to prove that $[\mathfrak{p}_2] \neq 1$, i.e., $\mathfrak{p}_2$ is not principal.

If $\mathfrak{p}_2$ was principal, then there would be an element $\beta \in \mathcal{O}_K$ with norm 2. Equivalently, there are $a, b \in \mathbb{Z}$ with the same parity such that $2 = (a^2 + 47b^2)/4$. The right hand side is too large if $b \neq 0$, so $a^2 = 8$ which is impossible. □

Since $x^2 - x + 12 \equiv x(x-1) \pmod 3$, we deduce that

$$3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3',$$

where $\mathfrak{p}_3 = (3, \theta)$ and $\mathfrak{p}_3' = (3, \theta - 1)$. The primes $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ each have norm 3.

Consider the ideal $(\theta) \subseteq \mathcal{O}_K$; this ideal has norm $(1+47)/4 = 12$. We have $\theta \in \mathfrak{p}_2$ and $\theta \in \mathfrak{p}_3$. We have $\theta \notin \mathfrak{p}_2'$ (since otherwise $1 = \theta - (\theta - 1) \in \mathfrak{p}_2'$). From this, we deduce that

$$(\theta) = \mathfrak{p}_2^2\mathfrak{p}_3.$$

In particular, $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-2}$ in Cl_K. Since $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$ and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$, we deduce that Cl_K is generated by $[\mathfrak{p}_2]$. From the above lemma, we conclude that Cl_K is a cyclic group of order 5.

(ii) Compute the class group of $\mathbb{Q}(\sqrt{-163})$.

Set $K = \mathbb{Q}(\sqrt{-163})$. We have $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-163})/2]$ and $\mathcal{O}_K$ has discriminant 163. The Minkowski bound for K is

$$M_K = \sqrt{163} \cdot 4/\pi \cdot 2!/2^2 < 9.$$

Therefore, the group Cl_K is generated by primes $\mathfrak{p}$ of $\mathcal{O}_K$ with norm at most 8 (and hence divides 2, 3, 5 or 7).

The order $\mathbb{Z}[\sqrt{-163}]$ has index 2 in $\mathcal{O}_K$. So for an odd prime $p \neq 163$, p is unramified in K and is inert if and only if -163 is not a square modulo p. An easy computations shows that -163 is not a square modulo $p \in \{3, 5, 7\}$. So there are no ideals with norm 3, 5 or 7.

We now deal with the primes dividing 2. The minimal polynomial of $(1+\sqrt{-163})/2$ is x^2-x+41. Since $x^2 - x + 41$ is irreducible modulo 2, we deduce that $2\mathcal{O}_K$ is a prime ideal.

Therefore, the class group of K is generated by the principal ideal $2\mathcal{O}_K$. Therefore, $\mathrm{Cl}_K = 1$ and hence K has class number 1.

(iii) Compute the class group of $\mathbb{Q}(\sqrt[3]{7})$.

Set $\theta = \sqrt[3]{7}$ and $K = \mathbb{Q}(\sqrt[3]{7})$. We claim that

$$\mathcal{O}_K = \mathbb{Z}[\theta];$$

we omit the proof it uses the ideas from homework 1. The discriminant of $\mathcal{O}_K$ is $-1323 = -3^3 7^2$. The Minkowski bound for K is

$$M_K = \sqrt{1323} \cdot 4/\pi \cdot 3!/3^3 < 10.5.$$

So Cl_K is generated by the prime ideals of norm at most 10 (and hence of norm 2, 3, 4, 5, 7, 8 or 9).

A direct computation shows that

$$N_{K/\mathbb{Q}}(a + b\theta + c\theta^2) = a^3 + 7b^3 + 49c^3 - 21abc$$

for all $a, b, c \in \mathbb{Z}$.

We have $x^3 - 7 \equiv (x+1)(x^2+x+1) \pmod 2$, so

$$2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2',$$

where $\mathfrak{p}_2 = (2, \theta+1)$ and $\mathfrak{p}_2 = (2, \theta^2+\theta+1)$. The ideals $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ have norm 2 and 4, respectively.

Lemma 2. *The group* Cl_K *is generated by* $[\mathfrak{p}_2]$.

Proof. • $p = 2$**:** We have $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$ since $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$.

• $p = 3$**:** Since $x^3 - 7 \equiv (x-1)^3 \pmod 3$, we have

$$3\mathcal{O}_K = \mathfrak{p}_3^3,$$

where $\mathfrak{p}_3 = (3, \theta - 1)$ is a prime ideal of norm 3.

Consider $\alpha := \theta - 1$. We have $N_{K/\mathbb{Q}}(\alpha) = 6$. By norm considerations, we have $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$ and hence $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$.

• $p = 5$**:** Since $x^3 - 7 \equiv (x+2)(x^2+3x+4) \pmod 5$, we have

$$5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5',$$

where $\mathfrak{p}_5 = (5, \theta+2)$ and $\mathfrak{p}_5' = (5, \theta^2+3\theta+4)$ are primes of norm 5 and 25, respectively.

Consider $\beta := -1 - \theta + \theta^2$. We have $N_{K/\mathbb{Q}}(\beta) = 20$. By norm considerations, the ideal (β) is either $\mathfrak{p}_5\mathfrak{p}_2^2$ or $\mathfrak{p}_5\mathfrak{p}_2'$. In either case, we find that $[\mathfrak{p}_5]$ is in the subgroup generated by $[\mathfrak{p}_2]$.

• $p = 7$**:** Since $x^3 - 7 \equiv x^3 \pmod 7$, we have

$$7\mathcal{O}_K = \mathfrak{p}_7^3,$$

where $\mathfrak{p}_7 = (7, \theta) = (\theta)$. We have $[\mathfrak{p}_7] = 1$.

Since Cl_K is generated by the prime ideals dividing 2, 3, 5 or 7, the above cases show that Cl_K is generated by $[\mathfrak{p}_2]$. □

It remains to compute the order of $[\mathfrak{p}_2]$. Consider $\alpha := 1 + \theta$. We have $N_{K/\mathbb{Q}}(\alpha) = 8$ and $\alpha \in \mathfrak{p}_2$. By norm considerations, the ideal (α) is $\mathfrak{p}_2^3$ or $\mathfrak{p}_2\mathfrak{p}_2' = 2\mathcal{O}_K$. Since $2 \nmid \alpha$, we deduce that $\mathfrak{p}_2^3 = (\alpha)$. In particular, $[\mathfrak{p}_2]^3 = 1$.

We now show that $[\mathfrak{p}_2] \neq 1$, i.e., $\mathfrak{p}_2$ is not principal. If $\mathfrak{p}_2$ was generated by a single element β, then $N_{K/\mathbb{Q}}(\beta) = \pm N(\mathfrak{p}_2) = \pm 2$, In particular, there would exist $a, b, c \in \mathbb{Z}$ such that

$$a^3 + 7b^3 + 49c^3 - 21abc = 2.$$

In particular, we would have $a^3 \equiv 2 \pmod 7$. A quick computation shows that this congruence has no solution and thus $[\mathfrak{p}_2] \neq 1$.

We have proved that Cl_K is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_2]$ has order 3. Therefore, Cl_K is a cyclic group of order 3.

Problem 2: Let K be a real quadratic field of discriminant D. Suppose that D is not a square modulo p for all prime $p \leq \sqrt{D}/2$ that are unramified in K. Prove that the class group Cl_K is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some r.

By the Minkowski bound, the class group Cl_K is generated by primes $\mathfrak{p} \subseteq \mathcal{O}_K$ with

$$N(\mathfrak{p}) \leq \sqrt{|\operatorname{disc} K|}(4/\pi)^s n!/n^n = \sqrt{D}/2.$$

Take any prime $\mathfrak{p}$ with $N(\mathfrak{p}) \leq \sqrt{D}/2$. Let $p \in \mathbb{Z}$ be the prime divisible by $\mathfrak{p}$; we have $p \leq N(\mathfrak{p}) \leq \sqrt{D}/2$.

• Suppose that p divides D. The prime p then ramifies in K and hence $\mathfrak{p}^2 = p\mathcal{O}_K$. In particular, $[\mathfrak{p}]$ has order 1 or 2 in Cl_K.
• Suppose that $p \nmid D$. The prime p is unramified in K so by the assumption of the problem, D is not a square modulo p; in particular, $p \neq 2$. Therefore, $x^2 - D$ is irreducible modulo p. This implies that $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ and hence $\mathfrak{p}$ is principal.

The finite abelian group Cl_K is generated by classes $[\mathfrak{p}]$ with $N(\mathfrak{p}) \leq \sqrt{D}/2$. From two cases above, we see that each such class $[\mathfrak{p}]$ has order 1 or 2. Therefore, Cl_K must be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some r.

Problem 3: Let $K \subseteq \mathbb{R}$ be a number field. Give necessary and sufficient conditions for the unit group $\mathcal{O}_K^\times$ to be dense in $\mathbb{R}$.

Let $\mathbb{R}_+$ be the multiplicative group of positive real numbers. Define the subgroup $U := \mathcal{O}_K^\times \cap \mathbb{R}_+$. Since $\mathcal{O}_K^\times = \pm U$ and $\mu_K = \{\pm 1\}$, the group U is a free abelian group of rank $r + s - 1$ (with our usual r and s).

Since $\mathcal{O}_K^\times = U \cup (-U)$, the group $\mathcal{O}_K^\times$ is dense in $\mathbb{R}$ if and only if U is dense in $\mathbb{R}_+$. The logarithm map $\log\colon \mathbb{R}_+ \to \mathbb{R}$ is an isomorphism of topological groups, so U is dense in $\mathbb{R}_+$ if and only if $\log(U)$ is dense in $\mathbb{R}$. The group $\log(U) \cong U$ is free abelian of rank $r + s - 1$

A discrete subgroup of $\mathbb{R}$ will be free abelian of rank at most 1 (in class, we proved more generality that a discrete subgroup of $\mathbb{R}^n$ is free abelian of rank at most n). Conversely, any subgroup of $\mathbb{R}$ generated by one element is discrete.

Putting everything together, we deduce that $\mathcal{O}_K^\times$ is discrete in $\mathbb{R}$ if and only if $r+s-1 \leq 1$. We have $r \geq 1$ since $K \subseteq \mathbb{R}$, we have $r+s-1 \leq 1$ if and only if $(r,s) \in \{(1,0),(2,0),(1,1)\}$. Recall that $[K:\mathbb{Q}] = r+2s$.

Therefore, $\mathcal{O}_K^\times$ is a discrete subgroup of $\mathbb{R}$ if and only if satisfies one of the following:

- $K = \mathbb{Q}$,
- K is a real quadratic field,
- K is a cubic field with a unique real embedding.

.

Problem 4: Prove the following theorem of Dirichlet using Minkowski's theorem.

Dirichlet's approximation theorem: For any $\alpha \in \mathbb{R}$ and integer $N \geq 1$, there are integers x and y such that $1 \leq y \leq N$, $\gcd(x,y) = 1$, and

$$\left|\alpha - \frac{x}{y}\right| \leq \frac{1}{Ny}.$$

Define the region

$$X := \{(x,y) \in \mathbb{R}^2 : |y\alpha - x| < 1/N,\ |y| < N+1\}$$

in $\mathbb{R}^2$. It is the interior of the parallelogram bounded by the lines $x = \alpha y + 1/N$, $x = \alpha y - 1/N$, $y = N+1$ and $y = -(N+1)$. It is convex, symmetric across 0, and has area $A := 2(N+1)\cdot 2(1/N) = 4 + 4/N$.

The covolume of the lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$, with the usual dot product, is 1. Since $A > 4 = 2^2\text{covol}(\mathbb{Z}^2)$, Minkowski's theorem implies that there is a non-zero point

$$(x,y) \in \mathbb{Z}^2 \cap X.$$

After replacing (x,y) by $(-x,-y)$, we may assume that $y \geq 0$. After replacing (x,y) by $(x/\gcd(x,y), y/\gcd(x,y))$, we may further assume that $\gcd(x,y) = 1$.

Since $(x,y) \in X$, we have $|y\alpha - x| < 1/N$ and $|y| < N+1$. Note that $y \neq 0$; if it did, then we would have $|x| < 1/N$, and hence $x = 0$, which would contradict $(x,y) \neq (0,0)$. Since y is a positive integer and $|y| < N+1$, we have $1 \leq y \leq N$.

Finally, dividing both sides of $|y\alpha - x| < 1/N$ by y gives $|\alpha - x/y| < 1/(Ny)$. This completes the proof of Dirichlet's approximation theorem.

Problem 5: Set $K := \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$. The "golden ratio" is $\varphi := (1+\sqrt{5})/2$; it is a fundamental unit of $\mathcal{O}_K^\times$. For each integer $n \geq 0$, let L_n and F_n be the integers satisfying

$$\varphi^n = \frac{L_n + F_n\sqrt{5}}{2}.$$

(i) Show that L_n and F_n are the Lucas and Fibonacci numbers, respectively (i.e., $L_0 = 2$, $L_1 = 1$, $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$ and $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$).

We have

$$\varphi^0 = \frac{2 + 0\cdot\sqrt{5}}{2} \quad \text{and} \quad \varphi^1 = \frac{1 + 1\cdot\sqrt{5}}{2}$$

and hence $L_0 = 2$, $L_1 = 1$, $F_0 = 0$ and $F_1 = 1$.

Now take any $n \geq 2$. The minimal polynomial of φ is $x^2 - x - 1$, so $\varphi^2 = 1 + \varphi$. Multiplying by φ^{n-2}, we have $\varphi^n = \varphi^{n-2} + \varphi^{n-1}$. Therefore,

$$\begin{aligned}\frac{L_n + F_n\sqrt{5}}{2} &= \varphi^n \\ &= \varphi^{n-2} + \varphi^{n-1} \\ &= \frac{L_{n-2} + F_{n-2}\sqrt{5}}{2} + \frac{L_{n-1} + F_{n-1}\sqrt{5}}{2} \\ &= \frac{(L_{n-2} + L_{n-1}) + (F_{n-2} + F_{n-1})\sqrt{5}}{2}.\end{aligned}$$

Since 1 and $\sqrt{5}$ are linearly independent over $\mathbb{Q}$. Therefore, $L_n = L_{n-2} + L_{n-1}$ and $F_n = F_{n-2} + F_{n-1}$ for all $n \geq 2$.

(ii) Take any integer $y \geq 1$. Show that y is a Fibonacci number if and only if $5y^2 - 4$ or $5y^2 + 4$ is a square.

First take any $n \geq 1$. We have $\frac{L_n + F_n\sqrt{5}}{2} = \varphi^n$ and hence

$$(L_n^2 - 5F_n^2)/4 = N_{K/\mathbb{Q}}(\frac{L_n + F_n\sqrt{5}}{2}) = N_{K/\mathbb{Q}}(\varphi)^n = \pm 1.$$

Therefore, $L_n^2 - 5F_n^2 = \pm 4$ and so $5F_n^2 + 4$ or $5F_n^2 - 4$ is a square.

Now suppose that y is a positive integer such that $5y^2 \pm 4 = x^2$ for some integer x; we may assume $x \geq 1$. We need to show that y is a Fibonacci number.

We have $x^2 - 5y^2 = \pm 4$ and hence

$$N_{K/\mathbb{Q}}\Big(\frac{x + y\sqrt{5}}{2}\Big) = \pm 1.$$

So $\frac{x+y\sqrt{5}}{2}$ is a unit in $\mathcal{O}_K^\times$ and is greater than 1 since x and y are positive. Therefore,

$$\frac{x + y\sqrt{5}}{2} = \varphi^n$$

for some $n \geq 1$ since φ is a fundamental unit. This implies that $y = F_n$ which is the n-th Fibonacci number by the previous part.

(iii) Prove that the solutions of $x^2 - 5y^2 = 1$ in positive integers are

$$(x, y) = (L_{6n}/2, F_{6n}/2)$$

with $n \geq 1$.

Let x and y be any solutions of $x^2 - 5y^2 = 1$ in positive integers. Then $x + y\sqrt{5}$ is an element of $\mathcal{O}_K^\times$ that is greater than 1. Therefore, $x + y\sqrt{5} = \varphi^n$ for some $n \geq 1$.

Now take any $n \geq 1$ and let x and y be the rational numbers satisfying $x + y\sqrt{5} = \varphi^n$. We have $x = L_n/2$ and $y = F_n/2$.

• We have

$$x^2 - 5y^2 = N_{K/\mathbb{Q}}(x + y\sqrt{5}) = N_{K/\mathbb{Q}}(\varphi)^n = (-1)^n,$$

and so $x^2 - 5y^2 = 1$ if and only if $n \equiv 0 \pmod 2$.

• Take n even. We now need to figure out for which n are x and y both integers. Since $x^2 - 5y^2 = 1$, this is equivalent to $y = F_n/2$ being an integer.

From the recursive equations defining the Fibonacci numbers, we find that F_n is even if and only if $n \equiv 0 \pmod 3$.

Therefore, the solutions of $x^2 - 5y^2 = 1$ in positive integers are $(L_n/2, F_n/2)$ with $n \geq 1$ divisible by 6.

Problem 6: Find three solutions $(a, b, c) \in \mathbb{Z}^3$ of

$$a^3 + 7b^3 + 49c^3 - 21abc = 1$$

with $c \neq 0$.
[Hint: $N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 7b^3 + 49c^3 - 21abc$ where $\alpha := \sqrt[3]{7}$ and $K = \mathbb{Q}(\alpha)$]

We first find a unit in $\mathcal{O}_K^\times - \{\pm 1\}$. It suffices to find $(a, b, c) \in \mathbb{Z}^3 \setminus \{(\pm 1, 0, 0)\}$ satisfying

$$N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 7b^3 + 49c^3 - 21abc = \pm 1.$$

By trial and error, I found the solution $(a, b, c) = (2, -1, 0)$. So

$$u := 2 - \alpha$$

is a unit in $\mathcal{O}_K^\times$. We have $N_{K/\mathbb{Q}}(u) = 2^3 + 7 \cdot (-1)^3 + 49 \cdot 0^3 - 21 \cdot 0 = 1$ and hence $N_{K/\mathbb{Q}}(u^n) = 1$ for all $n \geq 1$. The following is an easy computation:

$$\begin{aligned} u &= 2 - \alpha \\ u^2 &= 4 - 4\alpha + \alpha^2 \\ u^3 &= 1 - 12\alpha + 6\alpha^2 \\ u^4 &= -40 - 25\alpha + 24\alpha^2. \end{aligned}$$

Therefore, $(a, b, c) \in \{(4, -4, 1), (1, -12, 6), (-40, -25, 24)\}$ are solutions of $a^3 + 7b^3 + 49c^3 - 21abc = 1$.

Problem 7: Let K be a number field. Prove that there is a finite extension L/K such that for any ideal $I \subseteq \mathcal{O}_K$, the ideal $I \cdot \mathcal{O}_L$ of $\mathcal{O}_L$ is principal.

Let h be the cardinality of the class group of K (recall that the class group is finite!). Let $I_1, \ldots, I_h$ be non-zero ideals of $\mathcal{O}_K$ that represent all elements of the class group of K. Each ideal I_i^h is principal since the class group of K has order h; choose $\alpha_i \in \mathcal{O}_K$ for which $I_i^h = (\alpha_i)$.

Now consider a number field

$$L := K(\beta_1, \ldots, \beta_h),$$

where β_i satisfies $\beta_i^h = \alpha_i$ for all $1 \leq i \leq h$.

Take any ideal I of $\mathcal{O}_K$. We claim that $I\mathcal{O}_L$ is principal. This is trivial if $I = 0$, so we may assume that I is non-zero. Therefore, $I = cI_i$ for some $c \in K^\times$ and $1 \leq i \leq h$, and hence $I\mathcal{O}_K = c \cdot I_i\mathcal{O}_L$. To prove the claim, it thus suffices to show that $I_i\mathcal{O}_L$ is principal. However,

$$(I_i\mathcal{O}_L)^h = I_i^h\mathcal{O}_L = \alpha_i\mathcal{O}_L = \beta_i^h\mathcal{O}_L = (\beta_i\mathcal{O}_L)^h.$$

By the unique factorization of ideals in $\mathcal{O}_L$, we have $I_i\mathcal{O}_L = \beta_i\mathcal{O}_L$ and hence $I_i\mathcal{O}_L$ is principal as claimed.