HOMEWORK 2

Do at least 5 questions. Due November 6 at 11:59pm.

1. In this exercise, we show that every nonnegative integer is the sum of four squares.
This is trival for 0, 1, and 2, and there is an identity

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = (aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2 + (aC-bD+cA+dB)^2+(aD+bC-cB+dA)^2.$$

So we are reduced to showing that every odd prime p is the sum of four squares. Prove this via the following.

(a) Explain why the congruence $m^2+n^2+1 \equiv 0 \pmod{p}$ has a solutions in integers.
(b) Fix a solution n, m to the congruence in part (a), and let $\Lambda \subseteq \mathbb{Z}^4$ be the set of (a,b,c,d) such that $c \equiv ma+nb \pmod{p}$ and $d \equiv mb-na \pmod{p}$. Show that Λ is a lattice in $\mathbb{R}^4$ with covolume p^2.
(c) Use Minkowski's Theorem to show there is $(a,b,c,d) \in \Lambda$ such that $a^2+b^2+c^2+d^2 = p$.

2. Let F be a number field with ring of integers $\mathcal{O}_F$. For any nonzero ideal $I \subseteq \mathcal{O}_F$, show that $N(I) = |\mathcal{O}_F/I|$ extends to a homomorphism $N : \mathrm{Id}(\mathcal{O}_F) \to \mathbb{Q}^\times$, where $\mathrm{Id}(\mathcal{O}_F)$ is the group of fractional ideals of $\mathcal{O}_F$.

3. Determine all quadratic fields $F/\mathbb{Q}$ such that $\frac{1}{2}\left(\frac{4}{\pi}\right)^s \sqrt{|d_F|} < 2$, where d_F is the discriminant of F, $s=0$ if F is real quadratic, and $s=1$ if F is imaginary quadratic. Deduce that they all have class number 1.

4. Let $F/\mathbb{Q}$ be quadratic and write $F = \mathbb{Q}(\sqrt{d})$ with $d \neq 0, 1$ square free.

(a) Show that for any $p \mid d$, the ideal $P = (p, \sqrt{d})$ of $\mathcal{O}_F$ is prime and satisfies $P^2 = (p)$.
(b) Let $p_1, \dots, p_r$ be the distinct prime divisors of d. By part (a), we have prime ideals $P_1, \dots, P_r$ of $\mathcal{O}_F$ such that $P_i^2 = (p_i)$. Show that $P_1 \cdots P_r = (\sqrt{d})$.
(c) Assume that F is imaginary and let $P_1, \dots, P_r$ be as in part (b). Show that for any $1 \leq k < r$, the ideal $P_1 \cdots P_k$ is not principal. Deduce that $\mathrm{Cl}(F)$ contains a subgroup isomorphic to a product of $r-1$ cyclic groups of order 2.

5. Let F be a number field.

(a) Let $I \subseteq \mathcal{O}_F$ be a nonzero ideal. Show that if $n \geq 0$ is an integer such that $I^n = (a)$, then I generates a principal ideal in the ring of integers of $F(\sqrt[n]{a})$.
(b) Show that there is a finite extension E/F such that every fractional ideal I of F generates a principal fractional ideal of E.

6. Let A be a Dedekind ring with fraction field F. Let E/F be a finite separable extension, and let B be the integral closure of A in E. Let $b \in B$ be nonzero.

(a) Show that $\frac{\mathrm{N}_{E/F}(b)}{b} \in B$.
(b) Show that $b \in B^\times$ if and only if $\mathrm{N}_{E/F}(b) \in A^\times$.
(c) Give an example of a number field E and $0 \neq x \in E$ such that $\mathrm{N}_{E/\mathbb{Q}}(x) = \pm 1$ but $x \notin \mathcal{O}_E$.

7. Let F be a real quadratic field with discriminant $d = d_F$. Recall that d is either 0 or 1 mod 4. Fix some embedding $\sigma : F \hookrightarrow \mathbb{R}$ and using it identify F with $\mathbb{Q}(\sqrt{d})$.
(a) Explain why there is $\varepsilon \in \mathcal{O}_F^\times$ such that $\sigma(\varepsilon) > 1$ and is minimal with this property. Show that such an ε is a fundamental unit.
(b) Assume that there are solutions $a, b \in \mathbb{Z}$ to
$$a^2 - db^2 = -4.$$
Show that if $a, b \geq 1$ are minimal, then $\varepsilon = \frac{a+b\sqrt{d}}{2}$ is a fundamental unit.
(c) Assume that there are no solutions $a, b \in \mathbb{Z}$ to $a^2 - db^2 = -4$. Then show that there are solutions $a, b \in \mathbb{Z}$ to
$$a^2 - db^2 = 4,$$
and that if $a, b \geq 1$ are minimal, then $\varepsilon = \frac{a+b\sqrt{d}}{2}$ is a fundamental unit.

Definition. Let F be a number field. We say F is *totally real* if every embedding of F into $\mathbb{C}$ is a real embedding. We say F is *totally imaginary* if F has no real embeddings. We say F is *CM* if it is a totally imaginary quadratic extension of a totally real field.

8. Let E be a CM field with maximal totally real subfield F (so $[E : F] = 2$). Prove that the index of $\mu(E)\mathcal{O}_F^\times$ in $\mathcal{O}_E^\times$ is at most 2. (Hint: Let c be the nontrivial element of $\mathrm{Gal}(E/F)$ and consider the map $\varepsilon \mapsto \frac{c(\varepsilon)}{\varepsilon}$.)

9. Let F be a totally real number field. Let S be a proper nonempty subset of the embeddings $\{\sigma : F \hookrightarrow \mathbb{R}\}$. Show that there is $\varepsilon \in \mathcal{O}_F^\times$ such that $0 < \sigma(\varepsilon) < 1$ for all $\sigma \in S$ and $\sigma(\varepsilon) > 1$ for all $\sigma \notin S$. (Hint: Letting $n = [F : \mathbb{Q}]$, we know that $\mathrm{Log}(j(\mathcal{O}_F^\times))$ is a lattice in the trace zero subspace H of $\mathbb{R}^n$. Consider an appropriate translate an appropriate bounded region in H.)

10. Let A be a Dedekind ring with field of fractions F. Let E/F be a finite separable extension and let B be the integral closure of A in E. For a nonzero prime ideal Q of B dividing the prime ideal P of A, let $f(Q) = [B/Q : A/P]$ be the residue degree. Define a homomorphism $\mathrm{Nm}_{B/A} : \mathrm{Id}(B) \to \mathrm{Id}(A)$ by setting $\mathrm{Nm}_{B/A}(Q) = P^{f(Q)}$ if Q is a nonzero prime ideal of B and $Q \cap A = P$.
(a) Show that for $0 \neq x \in E$, we have $\mathrm{Nm}_{B/A}(xB) = \mathrm{Nm}_{E/F}(x)A$ (here xB denotes the principal fractional ideal generated by x, and similar notation for A).
(b) Show that if $A = \mathbb{Z}$ and E is a number field, then $\mathrm{Nm}_{\mathcal{O}_E/\mathbb{Z}}(I) = |\mathcal{O}_E/I|\mathbb{Z}$ for any nonzero ideal I of $\mathcal{O}_E$ (so $\mathrm{Nm}_{\mathcal{O}_E/\mathbb{Z}}$ recovers our previous definition of the absolute norm).

11. Let $F = \mathbb{Q}(\alpha)$ where $\alpha^3 = 2$. In what follows, you may use without proof that $\mathcal{O}_F = \mathbb{Z}[\alpha]$. Compute the prime factorizations, and the corresponding residue degrees, of 2, 3, 5, and 7 in $\mathcal{O}_F$.

12. Let $F = \mathbb{Q}(\zeta)$ where ζ is a primitive 5th root of 1. In what follows, you may use without proof that $\mathcal{O}_F = \mathbb{Z}[\zeta]$. Compute the prime factorizations, and the corresponding residue degrees, of 2, 3, 5, and 11 in $\mathcal{O}_F$.

13. Find all number fields F with $|d_F| \leq 12$.

We use the following notation and assumptions for next three problems. Let A be a Dedekind ring with fraction field F and let K/F and E/K be finite separable extensions with E/F Galois.

Let $P \subset A$ be a nonzero prime ideal and assume that for any prime Q of E above P, the residue extension $k(Q)/k(P)$ is separable.

14. (a) Prove that P is unramified in K if and only if $K \subseteq E^{I_Q}$ for every prime Q of E above P.
(b) Assume that E is the normal closure of K/F. Prove that P is unramified in K if and only if it is unramified in E.
(c) Let L/F be another subextension of E/F. Prove that if P is unramfied in both K and L if and only if it is unramified in the compositum KL.

Recall/learn that if G is a group, H and N are subgroups, and $g \in G$, then we can form the *double coset*

$$HgN = \{hgn \mid h \in H \text{ and } n \in N\}.$$

The double cosets partition G and the set of these double cosets is denoted $H\backslash G/N$. One can interpret this as the orbits of the left action of H on the left cosets G/N or as the orbits of the right action of N on the right cosets $H\backslash G$.

15. (a) Let $G = \mathrm{Gal}(E/F)$ and let $H = \mathrm{Gal}(E/K)$. Let Q be a prime above P in E. Show that the map $\sigma \mapsto \sigma(Q) \cap K$ induces a bijection from $H\backslash G/D_Q$ to the set of primes of K above P.
(b) Assume that E is the normal closure of K/F. Prove that P splits completely in K if and only if it splits completely in E.
(c) Let L/F be another subextension of E/F. Prove that P is totally split in both K and L if and only if it is totally split in the compositum KL.

16. Assume that P is unramified in E and that $k(P)$ is a finite field. Let Q be a prime of E above P, and let $\mathrm{Fr}_{Q/P}$ be the Frobenius at Q. Let $Q_K = Q \cap K$.
(a) Show that for any $\sigma \in \mathrm{Gal}(E/F)$, $\mathrm{Fr}_{\sigma(Q)/P} = \sigma\, \mathrm{Fr}_{Q/P}\, \sigma^{-1}$.
(b) Show that $\mathrm{Fr}_{Q/Q_K} = \mathrm{Fr}_{Q/P}^{f(Q_K/P)}$.
(c) Show that if K/F is Galois, then $\mathrm{Fr}_{Q_K/P} = \mathrm{Fr}_{Q/P}|_K$.
(d) Show that P is totally split in E if and only if $\mathrm{Fr}_{Q/P} = 1$.
(e) Show that P is inert in E if and only if $\mathrm{Fr}_{Q/P}$ generates $\mathrm{Gal}(E/F)$.

Remark. The first part of the above question implies that the conjugacy class of $\mathrm{Fr}_{Q/P}$ depends only on P. In particular, if $\mathrm{Gal}(E/F)$ is abelian, then the element $\mathrm{Fr}_{Q/P}$ depends only on P and not on Q. In this case, we denote it by Fr_P.

17. Let $F/\mathbb{Q}$ be quadratic and write $F = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree. Let p be an odd prime unramified in F and let $\mathrm{Fr}_p \in \mathrm{Gal}(E/F) \cong \{\pm 1\}$ be the Frobenius at p (see the remark above). Show that

$$\mathrm{Fr}_p = \begin{cases} 1 & \text{if } d \text{ is a square in } \mathbb{F}_p, \\ -1 & \text{if } d \text{ is not a square in } \mathbb{F}_p. \end{cases}$$

(This shows that Fr_p recovers the Legendre symbol $\left(\frac{d}{p}\right)$.)