Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 40 points' worth). Starred problems are especially recommended. Prepare to present 1-2 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 4)

1. [3pts] If a and b are relatively prime, show that $\mathbb{Q}(\zeta_{ab}) = \mathbb{Q}(\zeta_a, \zeta_b)$. Deduce that $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ for odd integers n. Do there exist distinct even integers $2m$ and $2n$ such that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_{2n})$?
2. [1pt] Suppose $K/\mathbb{Q}$ is a number field. Show that $K = \mathbb{Q}(\alpha)$ for some complex number α. [Hint: Apply the primitive element theorem.]
3. [1pt] Suppose $K/\mathbb{Q}$ is a number field. For any $\alpha \in K$, show that the minimal polynomial $m(x)$ of α is irreducible in $\mathbb{Q}[x]$.

0.1.2 Exercises from (Sep 5)

1. [1pt] Show that the set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.
2. [3pts*] Suppose D is squarefree. Show that the set of algebraic integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\sqrt{D}]$ when $D \equiv 2, 3 \pmod 4$ and that it is $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ when $D \equiv 1 \pmod 4$. [Hint: First verify that for $b \neq 0$ the minimal polynomial of $a + b\sqrt{D}$ is $m(x) = x^2 - 2a + (a^2 - Db^2)$, and then classify when the coefficients are integers.]
3. [2pts] For algebraic integers α and β, recall that if $\mathbb{Z}[\alpha]$ has basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $\mathbb{Z}[\beta]$ has basis $\{1, \beta, \dots, \beta^{m-1}\}$ then $\mathbb{Z}[\alpha, \beta]$ is spanned by $\{\alpha^i \beta^j\}_{1 \le i \le n, 1 \le j \le mn}$. By computing an appropriate determinant, use this observation to find a monic integer polynomial satisfied by $\sqrt{2} + \sqrt[3]{3}$ and by $\sqrt{2} \cdot (\sqrt[3]{3} - 1)$.
4. [1pt] Show that K is the fraction field of its ring of integers $\mathcal{O}_K$.
5. [1pt] For a separable extension K/F, show that the trace and norm as defined above are still Galois-invariant, that the trace is additive and F-linear, and that the norm is multiplicative.

0.1.3 Exercises from (Sep 9)

1. [2pts] Compute the four complex embeddings of $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ instead using the $\mathbb{Q}$-basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$, and find the trace and norm of $p + q\sqrt{2} + ri + si\sqrt{2}$.
2. [10pts*] Let K/F be an extension of number fields with $\alpha \in K$ and define $T_\alpha : K \to K$ to be the F-linear transformation of multiplication by α, namely with $T_\alpha(x) = \alpha x$ for all $x \in K$.
   (a) Show that the minimal polynomial of the linear transformation T_α is the minimal polynomial of the algebraic number α. [Hint: Show that $F[T_\alpha]$ is ring-isomorphic to $F[\alpha]$.]
   (b) Show that the eigenvalues of T_α in $\mathbb{C}$ are the elements $\sigma_i(\alpha)$, where $\sigma_1, \dots, \sigma_n$ are the complex embeddings of K fixing F.
   (c) Show that the characteristic polynomial $p(x) = \det(xI - T_\alpha)$ of T_α is $m(x)^{[K:F(\alpha)]}$ where $m(x)$ is the minimal polynomial of α over F.
   (d) Show that $\operatorname{tr}(T_\alpha) = \operatorname{tr}_{K/F}(\alpha)$ and that $\det(T_\alpha) = N_{K/F}(\alpha)$.
   (e) Use (a) and (d) to compute the trace, norm, and minimal polynomial of $\alpha = \sqrt[3]{2} + \sqrt{7}$ from $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{7})$ to $\mathbb{Q}$. [Suggestion: Compute the matrix T_α with respect to the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{7}, \sqrt[3]{2}\sqrt{7}, \sqrt[3]{4}\sqrt{7}\}$.]

0.1.4 Exercises from (Sep 11)

1. [2pts*] Show that when $D < 0$, the only units of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are ± 1, except in the case $D = -1$ with units $\pm 1, \pm i$ and in the case $D = -3$ with units $\pm 1, \pm \zeta_3, \pm \zeta_3^2$.
2. [2pts] Show that if K/F is a degree n-extension of number fields and $\mathcal{O}_F$ is a PID, then $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank n.

0.1.5 Exercises from (Sep 12)

1. [2pts] Use the result that any $\beta \in \mathcal{O}_K$ can be written as $\beta = \frac{1}{d}(c_1\alpha_1 + \cdots + c_n\alpha_n)$ for $d = \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ to prove directly that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

2. [1pt] Suppose G is isomorphic to $\mathbb{Z}^n$ and H is a subgroup of rank n. Show that G/H is isomorphic to a direct sum of n finite cyclic groups. [Hint: How many generators does it have?]

3. [2pts*] Show that for $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, if $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ is squarefree, then $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

0.1.6 Exercises from (Sep 16)

1. [2pts*] If $\alpha^3 + \alpha + 1 = 0$, show that the ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$. [Hint: Compute the discriminant.]

2. [1pt] Suppose α is algebraic of degree n over $\mathbb{Q}$. If $f(x), g(x) \in \mathbb{Q}[x]$ are such that $f(\alpha) = g(\alpha)$ and both f, g have degree less than n, show that $f(x) = g(x)$.

0.1.7 Exercises from (Sep 18)

1. [2pts] Show that the discriminant of the cubic polynomial $p(x) = x^3 + ax + b$ is $-4a^3 - 27b^2$.

2. [3pts*] Suppose $m(x) \in \mathbb{Z}[x]$ is monic, irreducible, and has squarefree discriminant. If α is any root of $m(x)$, prove that the ring of integers of $K = \mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$.

3. [3pts] Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{5})$ is $\mathbb{Z}[\sqrt[3]{5}]$. [Hint: First note $d_1 = 1$, then show $d_2 | 10$. Eliminate the possibility that d_2 is even, then show that $d_2 = 5$ leads to an eventual contradiction modulo 5.]

4. [3pts] Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{10})$ has integral basis $\{1, \sqrt[3]{10}, \frac{1 + \sqrt[3]{10} + \sqrt[3]{100}}{3}\}$. [Hint: First note $d_1 = 1$, then show $d_2 | 30$. Use traces to eliminate the possibility that d_2 is even or divisible by 5, and then conclude $d_2 = 3$.]

5. [3pts*] Show that the ring of integers of $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ has integral basis $\{1, \sqrt{3}, \frac{\sqrt{3} + \sqrt{7}}{2}, \frac{1 + \sqrt{21}}{2}\}$.

6. [3pts] Compute an integral basis for the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. [Hint: It's bigger than $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.]

0.2 Additional Exercises

1. [6pts*] Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n over $\mathbb{Q}$. The goal of this problem is to prove that if $|\sigma_i(\alpha)| = 1$ for all complex embeddings σ_i of K, then α is a root of unity. So suppose that $|\sigma_i(\alpha)| = 1$ for all complex embeddings σ_i of K.

   (a) If $m(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ is the minimal polynomial of α over $\mathbb{Q}$, show $|c_i| \le \binom{n}{i}$ for each i.

   (b) Show that there are only finitely many possible α.

   (c) Show that α must be a root of unity. [Hint: Consider the powers of α.]

2. [6pts] Let K be a number field of degree n over $\mathbb{Q}$ with complex embeddings $\sigma_1, \ldots, \sigma_n$, and with $\mathcal{O}_K$ having an integral basis $\alpha_1, \ldots, \alpha_n$. Consider the determinant D of the $n \times n$ matrix with (i, j)-entry $\sigma_i(\alpha_j)$. Expanding the determinant as a sum over all $n!$ permutations in S_n, let P be the sum of terms corresponding to even permutations and N be the sum of terms corresponding to odd permutations, so that $D = P - N$.

   (a) Show that $P + N$ and PN are both integers. [Hint: Show they are both Galois-invariant. Note that by working inside the Galois closure of K, one may view the σ_i as automorphisms.]

   (b) Deduce Stickelberger's criterion: that $\mathrm{disc}(K) = (P - N)^2 = (P + N)^2 - 4PN$ must be congruent to 0 or 1 modulo 4.