ALGEBRAIC NUMBER THEORY PROBLEMS

Please complete 20 of these problems. You can hand them in at any time.

The problems cover a lot of different areas of the course; thus some are more algebraic, some are more computational, etc. You can pick the problems that sound most appealing to you.

Unless it says otherwise, the computational problems are intended to be done by hand. Of course you can use pari-gp or something similar to check your answer or for calculator help . . . I just mean that the problems shouldn't be done using sophisticated functions in pari-gp.

Problems last modified: *Mon Mar 23 12:30:30 EDT 2015.*

(1) (a) Show that any quadratic number field has the form $\mathbb{Q}(\sqrt{m})$, where m is a squarefree integer.
   (b) Show that $\mathbb{Q}(\sqrt{m})$ is not isomorphic to $\mathbb{Q}(\sqrt{n})$ if m and n are distinct squarefree integers.

(2) Let F be the cubic field $\mathbb{Q}(\theta)$, where θ is a root of $x^3 - x - 4$.
   (a) Show that the index of the ring of integers in the $\mathbb{Z}[\theta]$ is at most 2.
   (b) Show that it is in fact 2 and find a basis of $\mathcal{O}_F$.

(3) Let p be an odd prime and let $\zeta_p = e^{2\pi i/p}$. Show that $\mathbb{Q}(\zeta_p)$ contains either $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$, and give conditions on p that determine which possibility occurs. Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ζ_p.

(4) Suppose m and n are distinct relatively prime squarefree integers and let $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. K is called a *biquadratic* field.
   (a) Find all subfields of K.
   (b) Assume m and n are congruent to 1 mod 4. Find the ring of integers of K.

(5) Milne, exercise 2-6.

(6) Milne, exercise 3-1.

(7) Milne, exercise 3-3.

(8) Suppose $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ is irreducible. Let α be a root of f.
   (a) Suppose $a^2 - 3b = d^2$ for some $d \in \mathbb{Q}$. Prove
   $$\operatorname{disc}(1, \alpha, \alpha^2) = -27 f(\frac{d-a}{3}) f(\frac{-d-a}{3}).$$
   (b) Show that this formula is true even if $d \notin \mathbb{Q}$.
   (c) Find the ring of integers of the field $\mathbb{Q}(\alpha)$ where $f = x^3 - 6x^2 + 9x + 3$.

(9) Consider the three cubic polynomials $x^3 - 18x - 6$, $x^3 - 36x - 78$, $x^3 - 54x - 150$.

(a) Show that these polynomials are irreducible over $\mathbb{Q}$.
(b) Show that the cubic fields F_1, F_2, F_3 defined by these polynomials have power bases for their rings of integers. Show that the discriminants of these three fields coincide and are all equal to 22356.
(c) Show that the fields F_1, F_2, F_3 are pairwise non-isomorphic.

(10) Milne, exercise 4-2.
(11) Milne, exercise 4-3.
(12) Milne, exercise 4-4.
(13) Milne, exercise 4-5.
(14) Milne, exercise 4-7.
(15) Milne, exercise 5-1.
(16) Milne, exercise 5-2.
(17) Milne, exercise 5-3.
(18) The totally positive region C of $K \otimes \mathbb{R} \simeq \mathbb{R}^r \otimes \mathbb{C}^s$ is the subset $(\mathbb{R}_{>0})^r \times \mathbb{C}^s$. A unit is called totally positive if it lies in C under the embedding $K \to K \otimes \mathbb{R}$. Let $U \subset \mathcal{O}^\times$ be the subgroup of totally positive units.
(a) Find generators for U where K is (i) the real quadratic field $\mathbb{Q}(\sqrt{7})$, (ii) the real cubic field of discriminant 49, and (iii) the complex cubic field of discriminant -23.
(b) The group U acts on C. Shintani proved that a there exists a finite collection of open rational simplicial cones $\Sigma = \{\sigma\}$ such that Σ is a fundamental domain for U in C. Find such a collection for the three fields in the first part.
(19) Prove that $\mathbb{Q}(\zeta_7)$ has class number 1, where ζ_7 is a primitive 7th root of 1. Do the same for the totally real subfield $\mathbb{Q}(\zeta_7)^+$, which has discriminant 49.
(20) (a) Find the ring of integers $\mathcal{O}$ of the biquadratic field $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.
(b) Show that $\mathcal{O}$ is a PID.
(c) Show that $\mathcal{O}$ contains the ring of integers of a quadratic field that is *not* a PID.
(21) Prove that $\mathbb{Z}[\alpha]$ is a PID, where $\alpha^3 = 2$.
(22) (a) Let $K/\mathbb{Q}$ be a number field and $I \subset \mathcal{O}$ an ideal. Show that there is a finite extension L/K such that I becomes principal in L. (Hint: some power of I, say I^m, is principal with generator $\alpha \in \mathcal{O}$. What happens if you adjoin $\sqrt[m]{\alpha}$ to K?)
(b) Show that there is a finite extension of K such that *every* ideal of $\mathcal{O}$ becomes principal.
(c) Find an extension of degree 4 for $K = \mathbb{Q}(\sqrt{-21})$ such that every ideal becomes principal (note that the class number of K is 4).
(23) A *pure cubic field* is one of the form $K = \mathbb{Q}(\sqrt[3]{m})$ where m is a cubefree integer.
(a) Find the rank of the unit group $\mathcal{O}_K^\times$ for a pure cubic field K.

(b) Let L/K be the normal closure of K. Show that $\mathcal{O}_K^\times$ is an infinite index subgroup of $\mathcal{O}_L^\times$.
(c) Show that L contains a unit of norm 1 that is not a root of unity. (Hint: look at things of the form $u/\bar{u}$, where the bar is complex conjugation.)