# 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. In addition to these problems, *any exercise in Milne can be treated as an assigned problem if you wish.* More precisely, I've only highlighted a few that I find appealling, but you can solve and submit any exercise in Milne as part of the 20.

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: *Wed Sep 6 14:22:50 EDT 2017.*

(1) Let $F = \mathbb{Q}(\zeta_{13})$, where $\zeta_{13}$ is a primitive 1th root of unity.
  (a) Find the lattice of all subfields of $F$ (i.e. find all fields and their inclusion relations).
  (b) For each subfield $E \subset F$, find a generating element $\theta$ such that $E = F(\theta)$ as a polynomial in $\zeta_{13}$.
  (c) For each $\theta$ you found, find an irreducible polynomial over $\mathbb{Q}$ for which it is a root.

(2) (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.

(3) Let $\mathcal{O}$ be the ring of integers in a number field $F$. Let $N\colon F \to \mathbb{Q}$ be the norm map. The ring $\mathcal{O}$ is called *(norm) Euclidean* if for each $a, b \in \mathcal{O}$, there exist $q, r \in \mathcal{O}$ such that $a = qb + r$ with either $r = 0$ or $N(r) < N(b)$. It is a basic fact from commutative algebra that $\mathcal{O}$ Euclidean implies $\mathcal{O}$ is a principal ideal domain and in fact a unique factorization domain. Note that there is a more general notion of Euclidean that allows "size" functions that aren't the norm, but here we take Euclidean to mean norm Euclidean.[1]
  (a) Show that the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ is Euclidean.
  (b) Show that the ring of integers in $\mathbb{Q}(\sqrt{-7})$ is Euclidean.
  (c) Show that the ring of integers in $\mathbb{Q}(\sqrt{-5})$ is not Euclidean.
  (d) Suppose $d$ is squarefree and is 1 or 2 mod 4. Show that if $d$ is sufficiently large, then $\mathbb{Z}[\sqrt{-d}]$ is not Euclidean.

[1] In fact, an imaginary quadratic field is Euclidean in this more general sense iff it is norm Euclidean. There are real quadratic fields that are Euclidean in the more general sense but not norm Euclidean, for example $\mathbb{Q}(\sqrt{69})$.

(4) Let $\alpha$ be algebraic over $\mathbb{Q}$ with monic minimal polynomial $f \in \mathbb{Q}[x]$ of degree $n$. Let $K = \mathbb{Q}(\alpha)$. Define the discriminant of the polynomial $f$ to be $d(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$, where the $\alpha_i$ are the distinct roots in an algebraic closure.
   (a) Show that $N_{K/\mathbb{Q}}(f'(\alpha)) = (-1)^{n(n-1)/2} d(f)$.
   (b) Show that if $f = x^3 + ax + b$, then $d(f) = -27b^2 - 4a^3$.

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

(6) 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 $\zeta_p$.

(7) Suppose $K$ and $L$ are two fields with integral bases $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ respectively. Suppose $[KL : \mathbb{Q}] = mn$ and that the discriminants of $K$ and $L$ are relatively prime. Show that $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is an integral basis for the compositum $KL$.

(8) 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 $K$. (Hint: Exercise (7).)

(9) Let $K$ be a number field. The *inverse different* is defined to be set of all $x \in K$ such that $\operatorname{Tr} xy \in \mathbb{Z}$ for all $y \in \mathcal{O}_K$.
   (a) Compute the inverse different of $K = \mathbb{Q}(\sqrt{-d})$ for $d > 0$ squarefree.
   (b) Show that the inverse different is a fractional ideal of $K$.
   (c) Show that the *inverse* of the inverse different is an ideal $\mathcal{D}$. This ideal is called . . . the *different*.
   (d) Compute the different for the imaginary quadratic fields.

(10) Milne, exercise 1-1.

(11) Milne, exercise 2-1.

(12) Milne, exercise 2-4.

(13) Milne, exercise 2-6.

(14) Milne, exercise 3-1.

(15) Milne, exercise 3-3.

(16) Milne, exercise 3-4.

(17) Suppose $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ is irreducible. Let $\alpha$ 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 $f = x^3 - 6x^2 + 9x + 3$.

(18) 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.

(19) Milne, exercise 4-2.
(20) Milne, exercise 4-3.
(21) Milne, exercise 4-4.
(22) Milne, exercise 4-5.
(23) Milne, exercise 4-7.
(24) Milne, exercise 5-1.
(25) Milne, exercise 5-2.
(26) Milne, exercise 5-3.

(27) 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 $\Sigma$ is a fundamental domain for $U$ in $C$. (If you are not sure what this means, just ask me.) Find such a collection for the three fields in the first part.

(28) Prove that $\mathbb{Q}(\zeta_7)$ has class number 1, where $\zeta_7$ is a primitive 7th root of 1. Do the same for the totally real subfield $\mathbb{Q}(\zeta_7)^+$, which has discriminant 49.

(29) Let $\mathcal{O}$ be the ring of integers of the biquadratic field $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ (cf. Exercise (7)).
- (a) Show that $\mathcal{O}$ is a PID.
- (b) Show that $\mathcal{O}$ contains the ring of integers of a quadratic field that is *not* a PID.

(30) Prove that $\mathbb{Z}[\alpha]$ is a PID, where $\alpha^3 = 2$.

(31) Show that $\mathbb{Z}[\sqrt{-14}]$ has class group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

(32) Let $f(x) = x^3 + 2x - 1$ and $K = \mathbb{Q}[x]/(f)$. Let $L = \mathbb{Q}(\sqrt{-59})$.
- (a) Show that $f$ is irreducible.
- (b) Show that the discriminant of $K$ is $-59$.

- (c) Find a polynomial giving the Galois closure $E$ of $K$. (Hint: use $L$).
- (d) The class number of $L$ is 3. Show that $E$ is the Hilbert class field of $L$.
- (e) Use a computer to find all examples like this. (There are finitely many imaginary quadratic fields with class number 3.)

(33) (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).

(34) 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.)

(35) (a) Show that if $\alpha$ is a root of a monic integral polynomial $f \in \mathbb{Z}[x]$, and if $f(r) = \pm 1$, then $\alpha - r$ is a unit in $\mathbb{Q}(\alpha)$. (Hint: Consider the polynomial $f(x+r)$.)
- (b) Find the fundamental unit in $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{7}$. (Hint: $\sqrt[3]{7} < 23/12$.)

(36) Let $F = \mathbb{Q}(\theta)$, where $\theta$ is a root of $x^4 - 3$.
- (a) Show that $F$ is not a normal extension of $\mathbb{Q}$.
- (b) Show that the extension $E/F$ given by taking the compositum of $F$ with $K = \mathbb{Q}(\sqrt{-1})$ is normal over $\mathbb{Q}$.
- (c) Find the Galois group of $E/\mathbb{Q}$.
- (d) Find all subfields of $E$.

(37) Carry out Exercise (36) for $F = \mathbb{Q}(\theta)$, where $\theta$ is a root of $x^5 - 3$. In other words, identify $K$, find $E$, and compute the Galois group and all subfields.

(38) Suppose that $p = 2^{2^k} + 1$ is a prime number. For example, $p = 3, 5, 17, 257, 65537$. Such primes are called *Fermat primes*, and only these five are known. Let us call an algebraic number $\alpha$ *constructible* if it can be obtained from the rationals through a finite process of the four basic arithmetic operations (+, −, ×, ÷) and taking square roots. Gauss used this notion to construct the regular 17-gon using compass and straightedge, hence the name constructible.

   (a) Show that the number $\cos(2\pi/p)$ is constructible if $p$ is a Fermat prime. (Hint: first construct $\exp(2\pi i/p)$. Use Galois theory.)
   (b) Explicitly $\cos(2\pi/p)$ as a constructible number for $p = 3, 5, 17$.

(39) Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be a biquadratic number field, where $p \neq q$ are prime.
   (a) Express the Dedekind zeta function of $K$ as a product of Dirichlet $L$-functions.
   (b) According to the Kronecker–Weber theorem, $K$ is a subfield of a cyclotomic field $E = \mathbb{Q}(\exp(2\pi i/N))$ for some $N$. Explicitly find $N$ realizing this result.