18.785 Number Theory **Fall 2015**

Problem Set #7 **Due: 11/04/2015**

Description

These problems are related to the material covered in Lectures 12-14. Your solutions are to be written up in latex (you can use the latex source for the problem set as a template) and submitted as a pdf-file with a filename of the form `SurnamePset7.pdf` via e-mail to `drew@math.mit.edu` by **5pm** on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references you consulted. If there are none, write "**Sources consulted: none**" at the top of your problem set. The first person to spot each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit.

Instructions: First do the warm up problems, then pick two of problems 1-5 to solve and write up your answers in latex. Anyone who wishes to do so may earn up to 25 points of extra credit by solving three problems (the extra credit you receive will be the worst of your three scores divided by 2). Finally, complete the survey problem 6.

Problem 0.

These are warm up problems that do not need to be turned in.

(a) Prove that the imaginary quadratic fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ all have class number 1 because the Minkowski bound is less than 2.

(b) Prove that the imaginary quadratic fields $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$ all have class number 1 because they have no ideals of prime norm below the Minkowski bound. Why is it enough to check only ideals of prime norm? Does this work for other number fields?

(c) Prove that there are no real cubic fields of absolute discriminant less than 20 and that every real cubic field of absolute discriminant at most M is generated by an algebraic integer with minimal polynomial $x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with $|a| < \sqrt{M} + 2$, $|b| < 2\sqrt{M} + 1$, and $|c| < \sqrt{M}$.

(d) Let $n \in \mathbb{Z}_{>0}$ and assume n^2-1 is squarefree. Prove $n+\sqrt{n^2-1}$ is the fundamental unit of $\mathbb{Q}(\sqrt{n^2-1})$.

Problem 1. A non-solvable quintic extension (50 points)

Let $f(x) := x^5 - x + 1$, let $K := \mathbb{Q}[x]/(f) =: \mathbb{Q}[\alpha]$ and let L be the splitting field of f.

(a) Prove that f is irreducible in $\mathbb{Q}[x]$, thus K is number field. Determine the number of real and complex places of K, and the structure of $\mathcal{O}_K^\times$ as a finitely generated abelian group (both torsion and free parts).

(b) Prove that the ring of integers of K is $\mathcal{O}_K := \mathbb{Z}[\alpha]$ and compute $\operatorname{disc}\mathcal{O}_K$, which you should find is squarefree. Use this to prove that for each prime p dividing $\operatorname{disc}\mathcal{O}_K$ exactly one of $\mathfrak{q}|p$ is ramified, and it has ramification index $e_\mathfrak{q} = 2$ and residue field degree $f_\mathfrak{q} = 1$. Conclude that $K/\mathbb{Q}$ is tamely ramified.

(c) Using the fact that any extension of local fields has a unique maximal unramified subextension, prove that for any monic irreducible polynomial $g \in \mathbb{Z}[x]$ the splitting field of g is unramified at all primes that do not divide the discriminant of g. Conclude that $L/\mathbb{Q}$ is unramified away from primes dividing $\operatorname{disc}\mathcal{O}_K$ and tamely ramified everywhere, and show that every prime dividing $\operatorname{disc}\mathcal{O}_K$ has ramification index 2. Use this to compute $\operatorname{disc}\mathcal{O}_L$.

(d) Show that $\mathcal{O}_K$ has no ideals of norm 2 or 3 and use this to prove that the class group of $\mathcal{O}_K$ is trivial and therefore $\mathcal{O}_K$ is a PID.

(e) Prove that $\operatorname{Gal}(L/\mathbb{Q}) \simeq S_5$, and that it is generated by the Frobenius elements σ_2 and σ_5 ($\operatorname{Gal}(L/\mathbb{Q})$ is nonabelian, so these are conjugacy class representatives).

Problem 2. Binary quadratic forms (50 points)

A *binary quadratic form* is a homogeneous polynomial of degree 2 in two variables:

$$f(x, y) = ax^2 + bxy + cy^2,$$

which we identify by the triple (a, b, c). We are interested in a specific set of binary quadratic forms, namely, those that are *integral* ($a, b, c \in \mathbb{Z}$), *primitive* ($\gcd(a, b, c) = 1$), and *positive definite* ($b^2 - 4ac < 0$ and $a > 0$). To simplify matters, in this problem we shall use the word *form* to refer to an integral, primitive, positive definite, binary quadratic form.

The *discriminant* of a form is the integer $D := b^2 - 4ac < 0$; although this is not necessary, for the sake of simplicity we restrict our attention to *fundamental discriminants* D, those for which D is the discriminant of $\mathbb{Q}[x]/(f(x, 1)) = \mathbb{Q}(\sqrt{D})$.

We define the (principal) *root* $\tau := \tau(f)$ of a form $f = (a, b, c)$ to be the unique root of $f(x, 1)$ in the upper half plane $\mathbb{H} := \{z \in \mathbb{C} : \operatorname{im} z > 0\}$:

$$\tau = \frac{-b + \sqrt{D}}{2a}.$$

Let $F(D)$ denote the set of forms with fundamental discriminant D, let $K = \mathbb{Q}(\sqrt{D})$, and let $\mathcal{O}_K$ be the ring of integers of K.

(a) For each form $f = (a, b, c) \in F(D)$ with root τ, define $I(f) := a\mathbb{Z} + a\tau\mathbb{Z}$. Prove that $\mathcal{O}_K = \mathbb{Z} + a\tau\mathbb{Z}$ and that $I(f)$ is a nonzero $\mathcal{O}_K$-ideal of norm a. Show that every nonzero fractional ideal J lies in the ideal class of $I(f)$ for some $f = (a, b, c) \in F(D)$.

(b) For each $\gamma = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f(x, y) \in F(D)$ define

$$f^\gamma(x, y) := f(sx + ty,\, ux + vy).$$

Show that $f^\gamma \in F(D)$, and that this defines a right group action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $F(D)$ (this means $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ acts trivially and $f^{(\gamma_1\gamma_2)} = (f^{\gamma_1})^{\gamma_2}$ for all $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$).

Call two forms $f, g \in F(D)$ *equivalent* if $g = f^\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(c) Prove that two forms $f, g \in F(D)$ are equivalent if and only if $I(f)$ and $I(g)$ represent the same ideal class in $\operatorname{cl}\mathcal{O}_K$.

Recall that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathbb{H}$ (on the left) via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d},$$

and that the set

$$\mathcal{F} = \{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in [-1/2, 0] \text{ and } |\tau| \geq 1\} \cup \{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in (0, 1/2) \text{ and } |\tau| > 1\}$$

is a fundamental region for $\mathbb{H}$ modulo the $\mathrm{SL}_2(\mathbb{Z})$-action. A form $f = (a, b, c)$ is said to be *reduced* if

$$-a < b \leq a < c \qquad \text{or} \qquad 0 \leq b \leq a = c.$$

(d) Prove that two forms are equivalent if and only if their roots lie in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, and that a form is reduced if and only if its root lies in $\mathcal{F}$. Conclude that each equivalence class in $F(D)$ contains exactly one reduced form.

(e) Prove that if f is reduced then $a \leq \sqrt{|D|/3}$; conclude that $\#\,\mathrm{cl}\,\mathcal{O}_K \leq |D|/3$.

Remark. The upper bound $|D|/3$ is an overestimate, in fact $\#\,\mathrm{cl}\,\mathcal{O}_K = O(|D|^{1/2} \log |D|)$; under the generalized Riemann hypothesis one can sharpen this to $O(|D|^{1/2} \log\log |D|)$.

(f) Compute the class numbers of $\mathbb{Q}(\sqrt{-103})$ and $\mathbb{Q}(\sqrt{-376})$ by enumerating the reduced forms in $F(D)$ and list reduced forms $f = (a, b, c)$ whose ideals $I(f)$ represent each element of the class group (you may wish to write a short Sage or Magma script to automate this task but this is not required).

Remark. One can define (as Gauss did) a composition law for forms corresponding to multiplication of ideals; the product of reduced forms need not be reduced, so one also needs an algorithm to reduce a given form, but this is easy. One can then compute the group operation in $\mathrm{cl}\,\mathcal{O}_K$ using composition and reduction of forms, and this process is quite efficient. Using the group operation one can compute $\#\,\mathrm{cl}\,\mathcal{O}_K$ much more efficiently than by enumerating reduced forms, and one can also compute the structure of $\mathrm{cl}\,\mathcal{O}_K$ as a finite abelian group.

Problem 3. Unit groups of real quadratic fields (50 points)

A (simple) *continued fraction* is a (possibly infinite) expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

with $a_i \in \mathbb{Z}$ and $a_i > 0$ for $i > 0$. They are more compactly written as $(a_0; a_1, a_2, \ldots)$. For any $t \in \mathbb{R}_{>0}$ the *continued fraction expansion* of t is defined recursively via

$$t_0 := t, \qquad a_n := \lfloor t_n \rfloor, \qquad t_{n+1} := 1/(t_n - a_n),$$

where the sequence $a(t) := (a_0; a_1, a_2, \ldots)$ terminates at a_n if $t_n = a_n$, in which case we say that $a(t) = (a_0; a_1, \ldots, a_n)$ is *finite*, and otherwise call $a(t) = (a_0; a_1, a_2, \ldots)$ *infinite*. If $a(t)$ is infinite and there exists $\ell \in \mathbb{Z}_{>0}$ such that $a_{n+\ell} = a_n$ for all sufficiently large n, we say that $a(t)$ is *periodic* and call the least such integer $\ell := \ell(t)$ the *period* of $a(t)$.

Given a continued fraction $a(t) := (a_0; a_1, a_2, \ldots)$ define the sequences of integers (P_n) and (Q_n) by

$$\begin{aligned} P_{-2} &= 0, & P_{-1} &= 1, & P_n &= a_n P_{n-1} + P_{n-2}; \\ Q_{-2} &= 1, & Q_{-1} &= 0, & Q_n &= a_n Q_{n-1} + Q_{n-2}. \end{aligned}$$

(a) Prove that $a(t)$ is finite if and only if $t \in \mathbb{Q}$, in which case $t = a(t)$.

(b) Prove that if $a(t) = (a_0; a_1, a_2, \ldots)$ is infinite then $(a_0; a_1, \ldots, a_n) = P_n/Q_n$ and $t_n = (a_n; a_{n+1}, a_{n+2}, \ldots)$ for all $n \geq 0$; conclude that $t = \lim_{n\to\infty} P_n/Q_n = a(t)$.

(c) Prove that $a(t)$ is periodic if and only if $\mathbb{Q}(t)$ is a real quadratic field.

Now let $D > 0$ be a squarefree integer that is not congruent to $1 \bmod 4$ and let $K = \mathbb{Q}(\sqrt{D})$. As shown on previous problem sets, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, and it is clear that $(\mathcal{O}_K^\times)_{\text{tors}} = \{\pm 1\}$. Every $\alpha = x + y\sqrt{D} \in \mathcal{O}_K^\times$ has $N(\alpha) = \pm 1$, and (x, y) is thus an (integer) solution to the *Pell equation*

$$X^2 - DY^2 = \pm 1 \tag{1}$$

(d) Prove that if (x_1, y_1) and (x_2, y_2) are solutions to (1) with $x_1, y_1, x_2, y_2 \in \mathbb{Z}_{>0}$ then $x_1 + y_1\sqrt{D} < x_2 + y_2\sqrt{D}$ if and only if $x_1 < x_2$ and $y_1 \leq y_2$, and show that $(x_1 + y_1\sqrt{D})^n > x_1 + y_1\sqrt{D}$ for all $n > 1$. Conclude that the fundamental unit $\epsilon = x + y\sqrt{D}$ of $\mathcal{O}_K^\times$ is the unique solution (x, y) to (1) with $x, y > 0$ and x minimal.

(e) Let $a(\sqrt{D}) = (a_0; a_1, a_2, \ldots)$, and define t_n, P_n, Q_n as above. Prove that

$$P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1} = \pm 1 \qquad \text{and} \qquad \frac{t_n P_{n-1} + P_{n-2}}{t_n Q_{n-1} + Q_{n-2}} = \sqrt{D}$$

for all $n \geq 0$. Use this to show that (P_{kl-1}, Q_{kl-1}) is a solution to (1) for all $k \geq 0$, where $\ell := \ell(\sqrt{D})$. Conclude that $\epsilon = P_{\ell-1} + Q_{\ell-1}\sqrt{D}$.

(f) Compute the fundamental unit ϵ for each of the real quadratic fields $\mathbb{Q}(\sqrt{19})$, $\mathbb{Q}(\sqrt{570})$, and $\mathbb{Q}(\sqrt{571})$; in each case give the period $\ell(\sqrt{D})$ as well as ϵ.

Problem 4. S-class groups and S-unit groups (50 points)

Let K be a number field with ring of integers $\mathcal{O}_K$, and let S be a finite set of places of K including all archimedean places. Define the *ring of S-integers* $\mathcal{O}_{K,S}$ as the set

$$\mathcal{O}_{K,S} := \{x \in K : v_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

(a) Prove that $\mathcal{O}_{K,S}$ is a Dedekind domain containing $\mathcal{O}_K$ with the same fraction field.

(b) Define a natural homomorphism between $\operatorname{cl} \mathcal{O}_{K,S}$ and $\operatorname{cl} \mathcal{O}_K$ (it is up to you to determine which direction it should go) and use it to prove that $\operatorname{cl} \mathcal{O}_{K,S}$ is finite.

(c) Prove that there is a finite set S for which $\mathcal{O}_{K,S}$ is a PID and give an explicit upper bound on $\#S$ that depends only on $n = [K : \mathbb{Q}]$ and $|\operatorname{disc} \mathcal{O}_K|$.

(d) Prove the *S-unit theorem*: $\mathcal{O}_{K,S}^\times$ is a finitely generated abelian group of rank $\#S - 1$.

Problem 5. Classification of global fields (50 points)

Let K be a field and let M_K be the set of places of K (equivalence classes of nontrivial absolute values). We say that K has a (strong) *product formula* if M_K is nonempty and there exists a set of representative $|\ |_v$ for $v \in M_K$ and a positive real numbers m_v such that for all $x \in K^\times$ we have

$$\prod_{v \in M_K} |x|_v^{m_v} = 1,$$

with all but finitely many factors in the product equal to 1. Equivalently, if we define *normalized absolute values* $\|\ \|_v := |x|_v^{m_v}$ for each $v \in M_K$, then for all $x \in K^\times$ we have

$$\prod_{v \in M_K} \|x\|_v = 1,$$

with $\|x\|_v = 1$ for all but finitely many $v \in M_K$.

Definition. A field K is a *global field* if it has a product formula and the completion of K at any nontrivial absolute value is a local field.

We proved in lecture that every finite extension of $\mathbb{Q}$ and $\mathbb{F}_q(t)$ is a global field. In this problem you will prove the converse (a theorem due to Artin and Whaples).

Let K be a global field and fix a set of normalized absolute values $\|\ \|_v$ for $v \in M_K$. As we defined in lecture, an M_K-*divisor* is a sequence of positive real numbers $c = (c_v)$ indexed by $v \in M_K$ with all but finitely many $c_v = 1$ such that for each $v \in M_K$ there is an $x \in K^\times$ for which $c_v = \|x\|_v$. We then define

$$L(c) := \{x \in K : \|x\|_v \le c_v \text{ for all } v \in M_K\}.$$

(a) Prove that M_K is infinite but contains only finitely many archimedean places.

(b) Prove that for every M_K-divisor c the set $L(c)$ is finite.

(c) Let F be a field. Prove that if K is a finite extension of F of if F is a finite extension of K then F is a global field.

(d) Prove that if M_K contains an archimedean place then K is a finite extension of $\mathbb{Q}$ (hint: show that K contains $\mathbb{Q}$ and use (b) to show that $K/\mathbb{Q}$ is a finite extension).

(e) Prove that if M_K does not contain an archimedean place then K is a finite extension of $\mathbb{F}_q(t)$ for some finite field $\mathbb{F}_q$ (hint: by choosing an appropriate M_K-divisor c, show that $L(c)$ is a finite field $k \subseteq K$ and that every $t \in K - k$ is transcendental over k; then show that K is a finite extension of $k(t)$ as in (d)).

(f) In your proofs of (a)-(e) above, where did you use the fact that the completions of K are local fields?

Problem 6. Survey

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			
Problem 5			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
10/29	Unit group and regulator				
11/3	Introduction to zeta functions				

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.