18.786 Number Theory II **Spring 2018**
Problem Set #1 **Due: 3/2/2018**

Description

These problems are related to the material covered in Lectures 1-5. Your solutions are to be written up in latex and submitted as a pdf-file with a filename of the form `SurnamePset1.pdf` via e-mail to `drew@math.mit.edu` by **noon** on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references 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: Pick any combination of problems to solve that sum to 100 and write up your answers in latex, then complete the survey problem 4.

Problem 0. Cohomological triviality (50 points)

Throughout this problem G is a finite group. A G-module A is said to by *acyclic* if $\hat{H}^n(G,A) = 0$ for all $n \in \mathbb{Z}$. It is *cohomologically trivial* if $\hat{H}^n(H,A) = 0$ for all subgroups $H \le G$ and all $n \in \mathbb{Z}$.

(a) Give an example of an acyclic G-module A that is not cohomologically trivial (hint: use a cyclic G), then show that induced G-modules $\operatorname{Ind}^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ are cohomologically trivial.

(b) Show that for any $\mathbb{Z}$-module R the G-module $R[G]$ (with G acting trivially on R and by left-multiplication on G) is cohomologically trivial, as is any free $R[G]$-module.

(c) Let G be a p-group and let A be a G-module of exponent dividing p. Show that if $H_1(G,A) = 0$ then A is free as an $\mathbb{F}_p[G]$-module, hence cohomologically trivial. Conclude that if $\hat{H}^n(G,A) = 0$ for any $n \in \mathbb{Z}$ then A is cohomologically trivial.

(d) Let G be a p-group and A a G-module with trivial p-torsion. Show the following are equivalent: (i) A is cohomologically trivial, (ii) $\hat{H}^n(G,A) = \hat{H}^{n+1}(G,A) = 0$ for some $n \in \mathbb{Z}$, (iii) A/pA is a free $\mathbb{F}_p[G]$-module.

(e) Show that a G-module A is cohomologically trivial if and only if it is cohomologically trivial as a G_p-module for every p-sylow subgroup G_p, equivalently, if and only if for each prime p dividing $\#G$ we have $\hat{H}^n(G_p,A) = \hat{H}^{n+1}(G_p,A) = 0$ for some p-Sylow subgroup G_p and some integer $n \in \mathbb{Z}$.

Problem 1. The cup product (50 points)

For G-modules A and B, let $A \otimes B$ denote the G-module $A \otimes_{\mathbb{Z}} B$ with diagonal G-action (so $g(a \otimes b) = ga \otimes gb$).

Definition. Let A and B be G-modules. The (cochain) *cup product* is the family of maps (indexed by integers $m,n \ge 0$)

$$C^m(G,A) \times C^n(G,B) \xrightarrow{\cup} C^{m+n}(G, A \otimes B)$$

defined by

$$(f_A \cup f_B)(g_1, \ldots, g_{m+n}) = f_A(g_1, \ldots, g_m) \otimes g_1 \cdots g_m f_B(g_{m+1}, \ldots, g_{m+n})$$

By Proposition 23.13, we can equivalently define the cup product as a map

$$\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{m+1}], A) \times \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{n+1}], B) \xrightarrow{\cup} \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{m+n+1}], A \otimes B)$$

defined by

$$(\varphi_A \cup \varphi_B)(g_0, \ldots, g_{m+n}) = \varphi_A(g_0, \ldots, g_m) \otimes \varphi_B(g_m, \ldots, g_{m+n})$$

which you may find easier to work with.

(a) Prove that for $f_A \in C(G, A)$ and $f_B \in C(G, B)$ we have

$$d^{m+n}(f_A \cup f_B) = (d^m(f_A) \cup f_B) + (-1)^m (f_A \cup d^n(f_B)),$$

where the d^* are coboundary maps.

(b) Show that the cochain cup product induces well defined maps in cohomology

$$H^m(G, A) \otimes_{\mathbb{Z}} H^n(G, B) \xrightarrow{\cup} H^{m+n}(G, A \otimes B),$$

and also in Tate cohomology for $m, n \geq 0$, and that for $m = n = 0$ this map is induced by the identity G-morphism on $A \otimes B$.

(c) Prove that the cup product is associative: $(x \cup y) \cup z = x \cup (y \cup z)$, and symmetric when mn is even and skew symmetric when mn is odd, that is $x \cup y = (-1)^{mn}(y \cup x)$. Hint: use dimension shifting (see Section 29.1).

(d) For $n \geq 0$ show that the isomorphism $\hat{H}^n(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{n+2}(G, A)$ given by Tate's Theorem (see Theorem 29.22) is the cup product with γ, where $H^2(G, A) = \langle \gamma \rangle$.

(e) Let G be a finite cyclic group and fix an isomorphism $\chi \colon G \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$. Construct a canonical isomorphism $\delta \colon \operatorname{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \to H^2(G, \mathbb{Z}/n\mathbb{Z})$ and show that for any G-module A and all $n \geq 0$, cup product with $\delta(\chi)$ defines an explicit isomorphism $\hat{H}^n(G, A) \xrightarrow{\sim} H^{n+2}(G, A)$ that depends only on the choice of χ (this provides a more explicit version of Theorem 23.33).

Problem 2. The local Hilbert symbol (50 points)

Let K be a local field whose characteristic is not 2.[1]

Definition. The *local Hilbert symbol* is the map $(\cdot, \cdot) \colon K^\times/K^{\times 2} \times K^\times/K^{\times 2} \to \{\pm 1\}$

$$(a, b) := \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } K, \\ -1 & \text{otherwise.} \end{cases}$$

Here $a, b \in K^\times$ are understood to represent elements of $K^\times/K^{\times 2}$, since we can absorb squares into x and y.

[1] Note that this excludes only extensions of $\mathbb{F}_2(t)$; extensions of $\mathbb{Q}_2$ are fine.

(a) Prove the Hilbert symbol is symmetric, bimultiplicative (so $(a, bc) = (a, b)(a, c)$) and nondegenerate (left kernel is trivial). Is this true if K is not a local field?

(b) Prove that for $a \notin K^{\times 2}$ we have $(a, b) = 1$ if and only if $b \in \mathrm{N}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$.

(c) For $a, b, c \in K^\times$ prove $ax^2 + by^2 = c$ has a solution if and only if $(-ab, c) = (a, b)$.

(d) For $a, b \in K^\times$ define the quaternion algebra $H_{a,b}$ as the K-algebra $K(i, j)$ with $i^2 = a$, $j^2 = b$, $ij = -ij$. Show that $(a, b) = 1$ if and only if $H_{a,b} \simeq \mathrm{M}_2(K)$, the 2×2 matrix algebra over K (such quaternion algebras are said to *split*).

(e) Show that $H_{a,b} \simeq H_{a,c}$ if and only if $[b] = [c]$ in $K^\times/N(K(\sqrt{a})^\times)$. Deduce that the isomorphism class of $H_{a,b}$ depends only on the Hilbert symbol (a, b).

Problem 3. Formal groups (100 points)

Let A be a commutative ring and for $F \in A[[X, Y]]$ consider the properties.

(1) $F(X, Y) = X + Y + (\deg \geq 2)$,

(2) $F(X, F(Y, Z)) = F(F(X, Y), Z)$,

that are satisfied by any formal group law over A, and in particular by

$$\mathbb{G}_a(X, Y) := X + Y, \qquad \text{and} \qquad \mathbb{G}_m(X, Y) := X + Y + XY.$$

The goal of this problem is to precisely characterize the rings A for which (1) and (2) are sufficient to define a formal group law (that is, they imply (3), (4), and (5) below). You will prove that this is true if and only if A contains no nonzero torsion nilpotents (which certainly applies to Lubin-Tate group laws, since then A is an integral ideal).

For any $F, G \in A[[X, Y]]$ (whether they are formal group laws or not), we define

$$\mathrm{Hom}(F, G) := \{f \in TA[[T]] : f(F(X, Y)) = G(f(X), f(Y))\},$$

and say that $\mathrm{Hom}(F, G)$ is nonzero if $\mathrm{Hom}(F, G) \neq \{0\}$.

(a) Show that if $F \in A[[X, Y]]$ satisfies (1) and (2) then it also satisfies:

(3) There is a unique $i_F \in XA[[X]]$ such that $F(X, i_F(X)) = 0$;

(4) $F(X, 0) = X$ and $F(0, Y) = Y$.

(b) Let $A := \mathbb{F}_p[\epsilon]/(\epsilon^2)$. Show that $F(X, Y) = X + Y + \epsilon XY^p$ satisfies (1), (2) but not

(5) $F(X, Y) = F(Y, X)$.

Now let A be any commutative ring that contains a nonzero torsion nilpotent. Show that for some $\epsilon \in A$ and prime p, we have $p\epsilon = 0 = \epsilon^2$, and $F(X, Y) = X + Y + \epsilon XY^p$ satisfies (1), (2) but not (5).

(c) Let $F \in A[[X, Y]]$ satisfy (1), (2). Show that there is a unique $\omega_F \in A[[T]]$ satisfying

$$\omega_F(F(T, S))F_X(T, S) = \omega_F(T), \qquad \omega_F(0) = 1,$$

where F_X is the formal partial derivative of $F(X, Y)$ with respect to X.

(d) Let A be a torsion free ring, put $K := A \otimes_{\mathbb{Z}} \mathbb{Q}$, and let $F \in A[[X,Y]]$ satisfy (1), (2). The *formal logarithm* $\log_F \in K[[T]]$ is the formal integral of ω_F with $\log_F(0) = 0$. Show that $\log_F(F(X,Y)) = \log_F(X) + \log_F(Y)$, and that there exists $\exp_F \in K[[T]]$ such that $\log_F \circ \exp_F = \exp_F \circ \log_F = T$. Conclude that $F(X,Y) = F(Y,X)$.

(e) Let $F \in A[[X,Y]]$ satisfy (1), (2), let $H(X,Y) := F(X, F(Y, i_F(X)))$, and show $H(X,Y) = Y + \sum_{i \geq 1} h_i(X) Y^i$ for some $h_i \in A[[X]]$. Let n be the least integer for which $h_n \neq 0$ or 0 if no such n exists. Prove that one of the following holds:

- $n = 0$ and $F(X,Y) = F(Y,X)$;
- $n = 1$ and $h_1 \in \mathrm{Hom}(F, \mathbb{G}_m)$;
- $n > 1$ and $h_n \in \mathrm{Hom}(F, \mathbb{G}_a)$.

(f) Let A be an integral domain and let $F, G \in A[[X,Y]]$ satisfy (1), (2). Show that if $\mathrm{Hom}(F,G)$ is nonzero and $G(X,Y) = G(Y,X)$ then $F(X,Y) = F(Y,X)$.

(g) Prove that there exists $F \in A[[X,Y]]$ satisfying (1), (2) but not (5) if and only if A contains a nonzero torsion nilpotent (Hint: consider the nilradical of A).

Problem 4. 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 0			
Problem 1			
Problem 2			
Problem 3			

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
2/7	Tate's Theorem				
2/12	Local Artin Reciprocity I				
2/14	Local Artin Reciprocity II				
2/20	Lubin-Tate formal group laws				
2/21	Local existence theorem				

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.