18.782 PROBLEM SET 2
DUE SUNDAY, OCTOBER 6, 2019

Please report any typos/mistakes in the problems to the instructor for bonus marks!

1. Hensel’s lemma.
   (a) Let \( f \in \mathbb{Z}_p[x] \) and suppose \(|f(a)|_p < |f'(a)|_p^2 \) for some \( a \in \mathbb{Z}_p \). Let \( a_1 = a \), and for \( n \geq 1 \) let
   \[
   a_{n+1} = a_n - f(a_n)/f'(a_n).
   \]
   Prove that this defines a Cauchy sequence \((a_n)\) in \( \mathbb{Z}_p \) whose limit \( b \) uniquely satisfies \( f(b) = 0 \) and \(|a - b|_p < |f'(a)|_p\), and moreover \(|f'(a)|_p = |f'(b)|_p\). (It may be helpful to work in terms of \( v_p \) and congruences modulo powers of \( p \).)

   (b) Let
   \[
   f(x, y, z) = ax^2 + by^2 + cz^2
   \]
   with \( a, b, c \in \mathbb{Z} \) and \( abc \neq 0 \) squarefree. (i) Using the stronger form of Hensel’s lemma obtained in part (a), show that \( f \) represents 0 in \( \mathbb{Q}_2 \) if and only if the congruence
   \[
   f(x, y, z) \equiv 0 \mod 8
   \]
   is solvable in integers with \( x, y, z \) with not all even. (ii) For an odd prime \( p \) dividing \( a \), give a necessary and sufficient congruence condition involving \(-bc\) (modulo \( p \)) for \( f(x, y, z) \) to represent 0 in \( \mathbb{Q}_p \).

   (c) Recall the subgroups \( U_n = 1 + p^n\mathbb{Z}_p \) of \( \mathbb{Z}_p^\times \). Modifying the argument we used to prove \( U_1 \simeq \mathbb{Z}_p \) if \( p \) is an odd prime, show that for \( p = 2 \) we have \( U_1 \simeq \{ \pm 1 \} \times U_2 \) and \( U_2 \simeq \mathbb{Z}_2 \). This structural result can be used to show that an element \( u \in \mathbb{Z}_2^\times \) is a square if and only if \( u \equiv 1 \mod 8 \). Give a direct proof of this latter fact using the stronger form of Hensel’s lemma above.

2. Quadratic forms and local-global principle.
   (a) Show that the Hasse-Minkowski theorem implies the following (apparently stronger) statement: given any \( a \in \mathbb{Q} \), a quadratic form \( q(x_1, \ldots, x_n) \) represents \( a \) over \( \mathbb{Q} \) if and only if it represents \( a \) over \( \mathbb{Q}_p \) for all \( p \leq \infty \).

   (b) Two quadratic forms \( q, q' \) over \( \mathbb{Q} \) are equivalent over \( \mathbb{Q} \) if and only if they are equivalent over \( \mathbb{Q}_p \) for all \( p \leq \infty \). Give a proof of this when \( q \) and \( q' \) are nondegenerate, using the Hasse-Minkowski theorem and Witt’s theorem.\(^1\) (Hint: First show that,\(^1\) Witt’s theorem states the following. Suppose that \( f(x_1, \ldots, x_n), g(x_1, \ldots, x_m), \) and \( h(x_1, \ldots, x_m) \) are nondegenerate quadratic forms over a field \( K \) of characteristic different from 2. Define \( f \oplus g \) to be the quadratic form \( f \oplus g(x_1, \ldots, x_{n+m}) := f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_{n+m}) \) in \( n + m \) variables, and similarly define \( f \oplus h \). If \( f \oplus g \) and \( f \oplus h \) are equivalent, then \( g \) and \( h \) are equivalent.)
if a quadratic form \( q(x_1, \cdots, x_n) \) over a field \( K \) of characteristic \( \neq 2 \) represents some nonzero \( a \in K \), then \( q \) is equivalent to a quadratic form of the shape
\[
a x_1^2 + q'(x_2, \cdots, x_n)
\]
where \( q' \) is some quadratic form in variables \( x_2, \cdots, x_n \).

3. **Affine varieties.** Let \( k \) be a field.

(a) For any ideals \( I, J \subseteq k[x_1, \cdots, x_n] \), prove or disprove:
   
   (i) \( V_{I \cap J} = V_{IJ} \).
   
   (ii) \( V_{I \cup J} = V_{I+J} \).

(b) Suppose \( f_1, \cdots, f_m \in k[x_1, \cdots, x_n] \) is a collection of polynomials such that
\[
(f_1, \cdots, f_m) = (1) = k[x_1, \cdots, x_n],
\]
so there exist \( g_1, \cdots, g_m \in k[x_1, \cdots, x_n] \) with \( 1 = \sum_{i=1}^m g_i f_i \). Then, for any choice of nonnegative integers \( a_1, \cdots, a_m \), we have
\[
(f_1^{a_1}, \cdots, f_m^{a_m}) = (1).
\]
Prove this in three ways:

(i) by explicitly describing elements \( h_i \in k[x_1, \cdots, x_n] \) such that \( 1 = \sum_{i} h_i f_i^{a_i} \);

(ii) by converting the problem to a topological statement about subsets on \( \mathbb{A}^n_k \);

(iii) by using the notion of radicals of ideals.

(c) If \( V \subseteq \mathbb{A}^n_k \) is an affine variety equipped with the Zariski topology, show that \( V \) is quasicompact, i.e. every open cover of \( V \) has a finite subcover.

(d) If \( f \in k[x_1, \cdots, x_n] \) is nonzero, then show that the open subvariety \( D_f = \mathbb{A}^n \setminus V_f \) has the structure of a closed affine subvariety of \( \mathbb{A}^{n+1} \). Use this to define the affine variety \( \text{GL}_n \) over \( \mathbb{Q} \) such that, for every field extension \( K/\mathbb{Q} \),
\[
\text{GL}_n(K) = \{ \text{set of invertible } n \times n \text{ matrices with coefficients in } K \}.
\]

(e) Give an example of an affine variety over a field \( K \) of characteristic zero such that \( V(L) \) is finite for every finite field extension \( L/K \) but \( V(K) \) is infinite.

(f) If \( f \subseteq k[x_1, \cdots, x_n] \) is an ideal generated by \( r \) elements, then show that \( V_f \subseteq \mathbb{A}^n_k \) has dimension \( \geq n - r \).

(g) The (prime) spectrum \( \text{Spec} \ A \) of a commutative ring \( A \) is the set of its prime ideals. Describe and draw a picture of \( \text{Spec} \mathbb{R}[x] \), and relate this to \( \text{Spec} \mathbb{C}[x] \).