EXERCISES AND SUPPLEMENTAL TOPICS FOR LECTURE 2

1. General exercises

Let F be a field of characteristic $\neq 2$.

(1) Let E be an extension of F (not necessarily finite!). Given a quadratic space (V, q), construct the quadratic space (V_E, q_E) where $V_E = V \otimes_F E$.
(2) Let $d \in F^\times \setminus F^{\times 2}$ and form the quadratic extension $F(\sqrt{d})$. Let (V, q) be a quadratic form over F which is anisotropic but such that $V \otimes_F F(\sqrt{d})$ is isotropic. Then show that V contains $\langle a, -ad\rangle$ as a summand for some $a \in F^\times$ (and conversely). (**Note**: this was incorrect in the earlier version; thanks to Niven Achenjang for the correction.)
(3) Let (V, q) be any two-dimensional quadratic space. Show that V is hyperbolic if and only if $\det V = -1 \in F^\times/F^{\times 2}$.
(4) Let (V, q) and (V', q') be two-dimensional quadratic spaces. Show that $(V, q) \simeq (V', q')$ if and only if they have the same determinant (in $F^\times/F^{\times 2}$) and they both represent a common element of F.
(5) Let (V, q) be a quadratic space and let $a \in F^\times$. Show that (V, q) represents a (i.e., there exists $v \in V$ with $v.v = a$) if and only if $V \oplus \langle -a\rangle$ is isotropic.
(6) Suppose the u-invariant of F is n (so every $(n+1)$-dimensional quadratic form over F is isotropic). Then for any n-dimensional quadratic space (V, q) over F, and any $a \in F^\times$, there exists $v \in V$ such that $v.v = a$. In lecture we used this fact for $n = 2$ (and $a = 1$).

2. Exercises on C_1 fields

(1) Let $\mathbb{F}_q$ be a finite field. Let $P(X_1, \ldots, X_n)$ be a homogeneous polynomial of degree d in n variables. Suppose $n > d$. Then there exists a nontrivial solution of $P(X_1, \ldots, X_n) = 0$ over $\mathbb{F}_q$. In fact, the number of all solutions including the trivial solution is $\equiv 0 \bmod p$ (Chevalley–Warning). Here p is the prime such that q is a power of p.
   (a) For $x \in \mathbb{F}_q$, we have $x^{q-1} = 1$ if $x \neq 0$.
   (b) The number of zeros of $P(X_1, \ldots, X_n)$ is congruent mod p to $-\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} P(x_1, \ldots, x_n)^{q-1}$ (note that this sum lives in $\mathbb{F}_q$).
   (c) For $i < q-1$, we have $\sum_{x\in\mathbb{F}_q} x^i = 0$ in $\mathbb{F}_q$.
   (d) Expand out the sum above. Each monomial in $P(X_1, \ldots, X_n)^{q-1}$ is of the form $cX_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$ with $\sum_i a_i = d(q-1)$. In particular, one of the a_i satisfies $a_i < q-1$, and deduce that the sum vanishes in $\mathbb{F}_q$.
   (e) Combine to deduce the claim.
(2) Let $P(X_1, \ldots, X_n)$ be a homogeneous polynomial of degree d in n variables over the function field $\mathbb{C}(t)$. If $d < n$, then $P(X_1, \ldots, X_n) = 0$ has a solution (special case of Tsen's theorem). In particular, any three-dimensional quadratic form over $\mathbb{C}(t)$ is isotropic.
   (a) Without loss of generality, suppose the coefficients of P are polynomials in $\mathbb{C}[t]$.

Date: July 13, 2021.

(b) Take $X_i = \sum_{j=0}^{m} a_{ij} t^j$ for some coefficients $a_{ij} \in \mathbb{C}$ and for some $m \gg 0$. In this case, the equation $P(X_1, \ldots, X_n) = 0$ can be regarded as a system of homogeneous polynomial equations over $\mathbb{C}$ in $n(m+1)$ variables. However, the number of equations needed is given by the number of degree $md + O(1)$. For $m \gg 0$, there are more variables than equations.

(c) Here we use the following basic fact: given r homogeneous polynomial equations in $\mathbb{C}^s$, if $r < s$, they have a nontrivial common root. Conclude the proof of the result.

3. The u-invariant

The *u-invariant* of a field F is the maximum dimension (or ∞) of an anisotropic quadratic form over F. For example, the u-invariant of $\mathbb{C}$ is 1, and we have seen that the u-invariant of $\mathbb{F}_q$ is 2. There are many open questions involving the u-invariant: for instance, it is not known what values it can take in general (it was once believed that the u-invariant has to be a power of two, but it is now known that all even values and some odd values are possible for the u-invariant). As another example, it is a consequence of the Hasse–Minkowski machinery that the u-invariant of $\mathbb{Q}(\sqrt{-1})$ is four, but it is not known what the u-invariant of the field of rational functions $\mathbb{Q}(\sqrt{-1})(t)$. See the survey article by Parimala, "A Hasse Principle for Quadratic Forms over Function Fields."

(1) Let $\mathbb{C}((t))$ be the Laurent series field of $\mathbb{C}$ (i.e., the fraction field of the ring of formal power series $\mathbb{C}[[t]]$). Show that any three-dimensional quadratic form over $\mathbb{C}((t))$ is isotropic. (In fact, any homogeneous polynomial equation of degree d in n variables for $n > d$ has a nontrivial solution.)

(2) More generally, show that the u-invariant of the Laurent series field $F((t))$ is twice the u-invariant of F (for any field F of characteristic $\neq 2$). You will use the fact that any element in $1 + tF[[t]]$ has a square root (why?).

4. The Cartan–Dieudonné theorem

Let (V, q) be a quadratic space over F. As in the lecture, we know that the orthogonal group $O(V, q)$ acts transitively on each of the level sets $\{v : q(v) = a\}$ for any $a \in k^\times$.

In this sequence of exercises we will prove the *Cartan–Dieudonné theorem*: any element of $O(V, q)$ is a product of $\leq n$ reflections, where $n = \dim V$.

(1) To begin with, prove the weaker assertion that any element $f \in O(V, q)$ is a product of some number of reflections. Use induction on $\dim V$. Given an anisotropic vector $v \in V$, show that (as in the lecture) there is a reflection $R : V \simeq V$ carrying $v \mapsto \pm fv$ (one of those). Inductively, show that $Rf : V \simeq V$ is a product of reflections and conclude.

(2) The argument in (1) does not quite manage to prove that any f is a product of $\leq n$ reflections; the issue is that given anisotropic vectors $v, w \in V$ with $v.v = w.w$, there need not exist a reflection R such that $Rv = w$. Such a reflection *does* exist if $v - w$ is anisotropic. Conclude that if V itself is anisotropic, then the argument of part (1) suffices to prove the Cartan–Dieudonné theorem.

(3) Now we start to prove the Cartan–Dieudonné theorem. By induction, we may assume the result in dimensions $< n$. The above arguments then show that f can be written as a product of $\leq n + 1$ reflections.

If there exists an anisotropic vector $v \in V$ with $v - fv$ either zero or anisotropic, then we can conclude the result for f by induction (why?). So, we may assume that *for every anisotropic $v \in V$, the vector $v - fv$ is isotropic but nonzero.*

(4) In general, any vector in any quadratic space is a "limit" of anisotropic vectors (why?). (Work over $F = \mathbb{C}$, where this literally makes sense, or one has to form some algebraic substitute of this.) Therefore, for *any* vector $v \in V$, $v - fv$ is isotropic. Let $M : V \to V$ be the transformation $\mathrm{id} - f$. Show that:
   - For any $v, w \in V$, we have $Mv.Mw = 0$, i.e., $(MV) \subset (MV)^{\perp}$.
   - Furthermore $\ker(M)$ (the fixed points of f) is a subspace consisting of isotropic vectors, and hence $\ker(M) \subset \ker(M)^{\perp}$.
   - Show also that $\ker M = (MV)^{\perp}$. Conclude that $M^2 = 0$.

(5) Use the inclusions $(MV) \subset (MV)^{\perp}$, $\ker(M) \subset \ker(M)^{\perp}$ and basic linear algebra to show that $\dim MV = \dim \ker M = \frac{n}{2}$ (in particular, n is even) and these inequalities are equalities.

(6) Using $M^2 = 0$, conclude that $f = \mathrm{id} - M$ has determinant 1.

(7) Using the inductive hypothesis on n, we saw that f is a product of $\leq n + 1$ reflections. Write f as such a product; if there are exactly $n+1$ reflections in the product, then obtain a contradiction since $\det f = 1$. This proves the theorem.