1. HYPERFIELDS

A hyperfield is an object like a field, but where the addition is allowed to be multivalued. Hyperfields and hyperrings were introduced by Marc Krasner, in 1956 and 1982, in connection with his work on valuations. The simplest examples of hyperrings are the quotient hyperrings.

Definition 1.1. If $S$ is a multiplicative subset of a ring $A$ (commutative with 1), the quotient hyperring $A/mS = (A/mS, +, -, 0, 1)$ is defined as follows: $A/mS$ is the set of equivalence classes with respect to the equivalence relation $\sim$ on $A$ defined by $a \sim b$ iff $as = bt$ for some $s, t \in S$. The operations on $A/mS$ are the obvious ones induced by the corresponding operations on $A$: Denote by $[a]$ the equivalence class of $a$. Then $[a] + [b] = [a + b]$, $[a] \cdot [b] = [ab]$, $-a = [s]$, and $0 = 0$, and $1 = 1$.

The above construction is not very interesting if $0 \in S$, so we usually assume $0 \notin S$. If $S$ is a multiplicative subset of a field $F$ and $0 \notin S$, then $F/mS = F/[S]$, where $[S] := \langle st^{-1} : s, t \in S \rangle$, the subgroup of $F^*$ generated by $S$. In this case, the quotient hyperring $F/mS = \{0\} \cup F^*/[S]$ is a hyperfield.

Definition 1.2. A hyperfield is a system $(A, +, \cdot, 0, 1)$ where $A$ is a set, $+$ is a multivalued binary operation on $A$, i.e., a function from $A \times A$ to the set of all subsets of $A$, $\cdot$ is a binary operation on $A$, $- : A \to A$ is a function, and $0, 1$ are elements of $A$ such that

I. $(A, +, \cdot, 0)$ is a canonical hypergroup, terminology as in J. Mittas 1969, i.e.,
   (1) $c \in a + b \Rightarrow a \in c + (-b)$,
   (2) $a \in b + 0$ iff $a = b$,
   (3) $(a + b) + c = a + (b + c)$, and
   (4) $a + b = b + a$; and

II. $(A, \cdot, 1)$ is a commutative monoid, i.e., $(ab)c = a(bc), ab = ba,$ and $a1 = a$ for all $a, b, c \in A$; and

III. $a0 = 0$ for all $a \in A$; and

IV. $a(b + c) = ab + ac$.

A hyperfield is a hyperring with $1 \neq 0$ such that every non-zero element has a multiplicative inverse.

Hyperrings form a category. A hyperring homomorphism from $A$ to $B$, where $A$, $B$ are hyperrings, is a function $\alpha : A \to B$ which satisfies $\alpha(a + b) \subseteq \alpha(a) + \alpha(b)$, $\alpha(ab) = \alpha(a)\alpha(b)$, $\alpha(-a) = -\alpha(a)$, $\alpha(0) = 0$, $\alpha(1) = 1$.

Here are some elementary consequences of the hyperring axioms: (i) $-0 = 0$ (ii) $-(a) = a$ (iii) $a + b \neq 0$ (iv) $\alpha(-b) = -(\alpha(b)$ (v) $(-\alpha)(-b) = \alpha(b)$.
M. Krasner seemed to be most interested in valued fields \((F, v)\) and quotient hyperfields of \(F\) of the form \(F/m(1 + I)\) where \(I\) is a proper ideal in the valuation ring of \(v\).

M. Krasner asked if every hyperring is realized as a subhyperring of a quotient hyperring of some ring. He also asked the same question for hyperfields. Counterexamples were produced by A. Nakassis 1988.

2. Quadratic Form Schemes

**Definition 2.1.** Let \(F\) be a field, char \(F \neq 2\). The quadratic form scheme of \(F\) is \(Q(F) := F/mF^2\) if \(F \neq \mathbb{F}_3, \mathbb{F}_5\). Here, \(F^{*2} := \{a^2 : a \in F^{*}\}\).

Thus \(Q(F)\) is a hyperfield, \(Q(F)^* = F^*/F^{*2}\). We assume always that char \(F \neq 2\), although sometimes we might forget to say it. For \(F \in \{\mathbb{F}_3, \mathbb{F}_5\}\) the definition of \(Q(F)\) is a bit different; see Remark 2.4 below.

**Example 2.2.**

(i) If \(F\) is algebraically closed, then \(Q(F) = \{0, 1\}\), with addition and multiplication defined by \(0 + a = a, 1 + 1 = \{0, 1\}, 0 \cdot a = 0, 1 \cdot 1 = 1\). In this example, \(-a = a\).

(ii) If \(F\) is real closed, then \(Q(F) = \{0, 1, -1\}\), with addition and multiplication defined by \(0 + a = a, 1 + 1 = 1, (-1) + (-1) = -1, 1 + (-1) = \{0, 1, -1\}, 0 \cdot a = 0, 1 \cdot 1 = (-1) \cdot (-1) = 1, 1 \cdot (-1) = -1\).

**Lemma 2.3.** Assume \(F \neq \mathbb{F}_3, \mathbb{F}_5\), \(a, b \in Q(F)\), \(a \neq 0\). Then

(i) \(a^2 = 1\).

(ii) \(b \in a + (-a)\).

(iii) \(a \in a + b\).

(iv) If \(a \neq -1\) then \(1 + a\) is a subgroup of \(Q(F)^*\).

**Proof.** Let \(a, b \in F\), \(a \neq 0\). (i) We want to show \(\overline{a}^2 = \overline{1}\). But this is clear: \(a^2 \in F^{*2}\), so \(\overline{a}^2 = \overline{a^2} = \overline{1}\). (ii) We want to show \(b \in \overline{a} + \overline{-a}\). Scaling, we are reduced to the case \(a = 1\). If \(b \neq \pm 1\), the identity \(b = \overline{(b+1)^2} - \overline{(b-1)^2}\) shows that \(\overline{b} \in \overline{1} + \overline{-1}\). Thus we are reduced to showing \(\overline{1} \overline{1} = \overline{1} + \overline{-1}\). Scaling, we are reduced further to showing \(\overline{1} \overline{1} = \overline{1} + \overline{-1}\). Since \(F \neq \mathbb{F}_3, \mathbb{F}_5\), char \(F \neq 2\), \(|F^{*}| \geq 6\), so there exists \(b \in F^*, b^2 \neq \pm 1\). Then \(b^2 = \overline{(\overline{b}+1)^2} - \overline{(\overline{b}-1)^2}\), so \(\overline{1} = \overline{b^2} = \overline{1} + \overline{-1}\). (iii) This is immediate from (ii). (iv) We want to show that if \(a \neq 0\), \(a \notin -F^{*2}\) then \(\overline{1} + \overline{a}\) is a subgroup of \(Q(F)^*\). Clearly \(0 \notin \overline{1} + \overline{a}\), so \(\overline{1} + \overline{a} \subseteq Q(F)^*\), \(\overline{1} + \overline{a} \subseteq Q(F)^*\) by (iii). Each \(\overline{b} \in Q(F)^*\) satisfies \(\overline{ab} = \overline{b^2} = \overline{1}\), so is its own inverse. Closure of \(\overline{1} + \overline{a}\) under multiplication follows from the standard identity

\[
(x_1^2 + ay_1^2)(x_2^2 + ay_2^2) = (x_1x_2 - ay_1y_2)^2 + a(x_1y_2 + x_2y_1)^2.
\]

\[\square\]

**Remark 2.4.** Lemma 2.3(iii) shows that, for \(a, b \in F^*\),

\[
(2.1) \quad \overline{a} + \overline{b} = \{\overline{x} \in F/mF^{*2} : \exists x, y \in F\} \text{ not both zero such that } c = ax^2 + by^2\}
\]

Unfortunately, this fails to hold for \(F \in \{\mathbb{F}_3, \mathbb{F}_5\}\). For \(F \in \{\mathbb{F}_3, \mathbb{F}_5\}\), it is necessary to modify the definition of addition in \(Q(F)\), defining \(\overline{a} + \overline{b}\) by equation (2.1) in this case, for \(a, b \neq 0\). Once this is done, one checks that \(Q(\mathbb{F}_3), Q(\mathbb{F}_5)\) are hyperfields, and Lemma 2.3 continues to hold for \(F \in \{\mathbb{F}_3, \mathbb{F}_5\}\).
Thus, \(F_3 = \{0, 1, 2\}\), \(F_3^2 = \{1\}\), so \(Q(F_3) = \{0, 1, 2\}\) with addition and multiplication defined by \(0 + a = a, 1 + 1 = 2 + 2 = \{1, 2\}\), \(0 \cdot a = 0, 1 \cdot 1 = 2 \cdot 2 = 1, 1 \cdot 2 = 2\). Similarly, \(F_5 = \{0, 1, 2, 3, 4\}\), \(F_5^2 = \{1, 4\}\), so \(Q(F_5) = \{0, 1, 2\}\) with addition and multiplication defined by \(0 + a = a, 1 + 1 = 2 + 2 = \{0, 1, 2\}\), \(1 + 2 = \{1, 2\}\). Note that, in \(Q(F_5)\), \(-1 = 2\) and \(-2 = 1\), whereas, in \(Q(F_3)\), \(-1 = 1\) and \(-2 = 2\).

**Definition 2.5.** An abstract quadratic form scheme is a hyperfield \(H\) satisfying (i), (ii) and (iv) of Lemma 2.3, i.e., for all \(a \in H^*\), (i) \(a^2 = 1\) (ii) \(a + (-a) = H\) and (iv) if \(a \neq -1\) then \(1 + a\) is a subgroup of \(H^*\).

Given an abstract quadratic form scheme \(H\), it is natural to wonder if there exists a field \(F\), \(\text{char } F \neq 2\), with \(H \cong Q(F)\)? This question seems to have been considered first by L. Szczepanik around 1980. Surprisingly, this question is still open. The answer is known to be ‘yes’ for \(|H^*| \leq 32\). In this situation the number of (non-isomorphic) quadratic form schemes is also known:

| \(|H^*|\) | 1 | 2 | 4 | 8 | 16 | 32 |
|---------|---|---|---|---|----|----|
| \# of quadratic form schemes | 1 | 3 | 6 | 17 | 51 | 155 |

The proof is quite complicated. One part of the proof involves classifying all abstract quadratic form schemes with \(|H^*| \leq 32\). This was accomplished in several papers by various authors 1979-1985. The other part involves using valuation theory to show that all of the abstract quadratic form schemes obtained in this classification are realized as quadratic form schemes of fields; see M. Kula 1979.

### 3. Witt equivalence

**Definition 3.1.** Two fields \(F_1, F_2\) of characteristic \(\neq 2\) are said to be Witt equivalent, denoted \(F_1 \sim F_2\), if their quadratic form schemes are isomorphic, i.e., \(Q(F_1) \cong Q(F_2)\).

Why is one interested in Witt equivalence? In 1937 Ernst Witt initiated the study of quadratic forms over an arbitrary field \(F\) of characteristic \(\neq 2\). He assigned to the field \(F\) a ring \(W(F)\), the so-called Witt ring of \(F\), which encodes the theory of quadratic forms over \(F\). Thus, if \(F_1\) and \(F_2\) are fields having isomorphic Witt rings, then their quadratic form theories are the same. It follows from a result of D.K. Harrison 1970 that \(W(F_1) \cong W(F_2)\) iff \(Q(F_1) \cong Q(F_2)\). Consequently, \(Q(F)\) also encodes the theory of quadratic forms over \(F\), i.e., Witt equivalent fields have the same quadratic form theory. At the same time, \(Q(F)\) is much simpler and easier to work with than \(W(F)\).

**Example 3.2.**

(i) \(F \sim \mathbb{C}\) iff \(F^* = F^{*2}\).

(ii) \(F \sim \mathbb{R}\) iff \(F^{*2}\) is an ordering of \(F\), i.e. \(F^* = F^{*2} \cup -F^{*2}\) (disjoint union) and \(F^{*2}\) is closed under addition.

**Example 3.3 (Finite Fields).** Suppose \(F\) is a finite field, \(\text{char } F \neq 2\).

Claim: \(|Q(F)^*| = 2\). Define \(\alpha : F^* \to F^*\) by \(\alpha(a) = a^2\). \(\alpha\) is a group homomorphism, \(a^2 = 1\) iff \(a = \pm 1\), so \(\alpha(2) = 2\). Thus \(|F^{*2}| = \frac{|F^*|}{2}\), so \(\left|\frac{F^*}{2}\right| = \frac{|F^*|}{|F^{*2}|} = 2\). This proves the claim.

Suppose now that \(-1 \neq 1\) in \(Q(F)\) (i.e., that \(-1\) is not a square in \(F^*\)). Then \(Q(F) = \{0, 1, -1\}\), \(0 + a = a, 1 + 1 = 1, -1 \in (-1) + (-1)\) (by Lemma 2.3(iii)),
For any finite field $F$, let $Q$ denote by $F$ square in $F$. In this case.

Suppose now that $-1 = 1$ in $Q(F)$. Then $Q(F) = \{0, 1, p\}$ for some $p$. Arguing in a similar way as before we see that $0 + a = a, 1 + p = \{1, p\}$ (by Lemma 2.3(ii)), $1 + 1 = 1 + 1 = \{1, -1\}$. A similar argument shows that $1 + (-1) = \{1, -1\}$. It follows that $Q(F) \cong Q(F_3)$ in this case.

Finally, recall that the multiplicative group of a finite field is cyclic, so $-1$ is a square in $F^*$ iff $|F| - 1$ is divisible by 4.

In summary, we have proved:

**Theorem 3.4.** For any finite field $F$, char $F \neq 2$,

$$F \cong \begin{cases} F_3 & \text{if } |F| \equiv 3 \pmod{4} \\ F_5 & \text{if } |F| \equiv 1 \pmod{4} \end{cases}.$$ 

4. HENSELIAN VALUED FIELDS

In this section we assume $(F, v)$ is a Henselian valued field, char $F \neq 2$. We denote by $F_v$ the residue field of $(F, v)$. There are two cases to consider:

(i) the dyadic case: char $F_v = 2$.

(ii) the non-dyadic case: char $F_v \neq 2$.

Here we only consider the non-dyadic case, which is much easier. Actually, we don’t need the full strength of the Henselian assumption for what we do here. All we need is that every element of $F$ of the form $1 + x$, $v(x) > 0$, has a square root in $F$.

Denote by $A_v$ the valuation ring of $v$ and by $M_v$ and $U_v$ maximal ideal and unit group of $A_v$. Denote by $\pi: A_v \rightarrow F_v$ the natural ring homomorphism (so $M_v = \ker(\pi)$). The groups $U_vF_v^2/F_v^2$ and $F_v^*/F_v^2$ are naturally isomorphic via the map $\alpha: U_vF_v^2/F_v^2 \rightarrow F_v^*/F_v^2$ defined by $uF_v^2 \mapsto \pi(u)F_v^2, u \in U_v$. The point is that if $uF_v^2$ is in the kernel of $\alpha$ then there exists $w \in U_v$ such that $\pi(u/w^2) = 1$. Thus $u/w^2 \in 1 + M_v \subseteq F_v^2$, so $u \in F_v^2$. There is a natural surjective group homomorphism $\beta: F^*/F_v^2 \rightarrow v(F^*)/2v(F^*)$ with kernel equal to $U_vF_v^2/F_v^2$, defined by $xF_v^2 \mapsto v(x) + 2v(F^*)$. Combining these two facts yields a natural short (split) exact sequence

$$0 \rightarrow F^*_v \xrightarrow{\beta} F^*/F_v^2 \xrightarrow{\alpha^{-1}} F_v^*/F_v^2 \rightarrow 0.$$ 

**Theorem 4.1.** Let $(F, v)$ be a non-dyadic Henselian valued field. Then

(i) There is a natural hyperfield embedding $i: Q(F_v) \rightarrow Q(F)$.

(ii) Every $a \in Q(F) \setminus iQ(F_v)$ is rigid, i.e. $1 + a = \{1, a\}$.

**Proof.**

(i) The map $i$ is defined as follows: If $a \neq 0$ then $i(a) := \alpha^{-1}(a)$. If $a = 0$ then $i(0) := 0$. The image of $Q(F_v)$ under $i$ is $\{0\} \cup U_vF^*/F^*$. It is clear that $i(0) = 0$, $i(1) = 1$, $i(ab) = i(a)i(b)$, $i(-a) = -i(a)$ and $i(0 + a) = i(0) + i(a)$. One can show that $i(a + b) = i(a) + i(b)$ if $a, b \neq 0, b \neq -a$. This is left as an exercise. Observe
that if $a, b \neq 0, b = -a$, then $a + b = Q(F_v)$, $i(a) + i(b) = Q(F)$, (by Lemma 2.3(i)), so typically $i(a + b) \neq i(a) + i(b)$ in this case.

(ii) We want to show that if $a \in F^+ \setminus U_v F^{+2}$ then $\bar{T} + \bar{x} = \{ \bar{T}, \bar{x} \}$. The inclusion $\{ \bar{T}, \bar{x} \} \subseteq \bar{T} + \bar{x}$ is clear; it follows from Lemma 2.3(iii). The other inclusion follows from the fact that if $c = x^2 + ay^2$, $x, y \in F^*$, then $v(x^2) \neq v(ay^2)$. If $v(x^2) < v(ay^2)$ then $c = x^2(1 + ay^2/x^2) \in x^2(1 + M_v) \subseteq F^{+2}$, so $\bar{c} = \bar{T}$. If $v(x^2) > v(ay^2)$ then $c = ay^2(1 + x^2/ay^2) \in ay^2(1 + M_v) \subseteq F^{+2}$, so $\bar{c} = \bar{x}$. \hfill \Box

**Remark 4.2.**

(i) It follows from Theorem 4.1 that the hyperfield $Q(F)$ is completely determined by the hyperfield $Q(F_v)$ and the group $v(F^*)/2v(F^*)$. One says that $Q(F)$ is a group extension of $Q(F_v)$ by the group $v(F^*)/2v(F^*)$ to describe this situation.

(ii) Specifically, if $a, b \in Q(F)$,

$$a + b = \begin{cases} a & \text{if } b = 0 \\ Q(F) & \text{if } a, b \neq 0, b = -a \\ a(1 + ba^{-1}) = a(1, ba^{-1}) = \{ a, b \} & \text{if } a, b \neq 0, ba^{-1} \not\in \bar{i}Q(F_v) \\ a(1 + ba^{-1}) = a(1 + i^{-1}(ba^{-1})) & \text{if } a, b \neq 0, ba^{-1} \in \bar{i}Q(F_v), b \neq -a \\ \end{cases},$$

(iii) Theorem 4.1 was proved first in the context of Witt rings. The corresponding result for Witt rings asserts that $W(F)$ is isomorphic to $W(F_v)[v(F^*)/2v(F^*)]$ (the group ring of the group $v(F^*)/2v(F^*)$ with coefficients in the ring $W(F_v)$). In the case where the valuation $v$ is discrete rank one this was proved first by T.A. Springer 1955. Observe that, in this special case, $v(F^*)/2v(F^*) = \mathbb{Z}/2\mathbb{Z}$, a cyclic group of order 2.

5. **Local fields**

**Definition 5.1.** A local field, by definition, is a complete discrete valued field with finite residue field.

A characteristic zero local field is a finite extension of $\mathbb{Q}_p$ (the $p$-adic completion of $\mathbb{Q}$), for some prime $p$. A characteristic $p$ local field is a field of the form $\mathbb{F}_q((t))$, $q = p^f, f \geq 1$.

In view of Theorems 3.4 and 4.1, the non-dyadic local case is fairly straightforward:

**Theorem 5.2.** Let $(F, v)$ be a nondyadic local field. Then

$$F \sim \begin{cases} \mathbb{Q}_3 & \text{if } |F_v| \equiv 3 \mod 4 \\ \mathbb{Q}_5 & \text{if } |F_v| \equiv 1 \mod 4 \\ \end{cases}.$$

**Proof.** If $|F_v| \equiv 3 \mod 4$ then $Q(F_v) \cong Q(\mathbb{Q}_3)$. Then $Q(F)$ and $Q(\mathbb{Q}_3)$ are group extensions of $Q(\mathbb{F}_3)$, each by a cyclic group of order 2, so $Q(F) \cong Q(\mathbb{Q}_3)$. Similarly, if $|F_v| \equiv 1 \mod 4$ then $Q(F_v) \cong Q(\mathbb{Q}_5)$. Then $Q(F)$ and $Q(\mathbb{Q}_5)$ are group extensions of $Q(\mathbb{F}_5)$, each by a cyclic group of order 2, so $Q(F) \cong Q(\mathbb{Q}_5)$. \hfill \Box

If $F$ is a nondyadic local field then, computing using equation (4.1), we see that

$$|Q(F^*)| = |F^*/F^{*2}| = |F_v^*/F_v^{*2}| \cdot |\mathbb{Z}/2\mathbb{Z}| = 2 \cdot 2 = 4.$$

Dyadic local fields are finite extensions of $\mathbb{Q}_2$. For dyadic local fields the situation is more complicated.
Theorem 5.3. Suppose $F$ is a finite extension of $\mathbb{Q}_2$, $[F : \mathbb{Q}_2] = n$. Then

(i) $|Q(F)^*| = 2^{n+2}$.

(ii) For $a \in Q(F)^*$, $a \neq -1$ the group $1 + a$ has index 2 in $Q(F)^*$.

(iii) If $n$ is odd then the Witt equivalence class of $F$ depends only on $n$. If $n$ is even then there are exactly two Witt equivalence classes: one with $\sqrt{-1} \in F$ and one with $\sqrt{-1} \notin F$.

Proof. Omitted.

6. Behaviour of orderings and valuations under Witt equivalence

Let $F$ be a field, char $F \neq 2$. How much of $F$ can be ‘seen’ from the viewpoint of the quadratic form scheme of $F$? It turns out that all orderings of $F$ can be seen, and that certain non-dyadic valuations of $F$ can also be seen. We explain this now.

Recall that an ordering of a field $F$ is a subset $P$ of $F^*$ such that $F^* = P \cup -P$ (disjoint union), $P \cdot P \subseteq P$, $P + P \subseteq P$. If $P$ is an ordering of $F$ then $F^{*2} \subseteq P$ and $P$ is a subgroup of $F^*$.

Denote by $Q_2$ the quadratic form scheme of $\mathbb{R}$ (or of any real closed field). Thus $Q_2 = \{0, 1, -1\}$ with addition and multiplication satisfying: $0 + a = a$, $1 + 1 = 1$, $(-1) + (-1) = -1$, $1 + (-1) = \{0, 1, -1\}$, $0 \cdot a = a$, $1 \cdot 1 = (-1) \cdot (-1) = 1$, $1 \cdot (-1) = -1$.

Theorem 6.1. Let $F$ be a field, char $F \neq 2$. The set of orderings of $F$ is in natural one-to-one correspondence with the set of hyperring homomorphisms $\alpha : Q(F) \to Q_2$.

Proof. If $P$ is an ordering of $F$ then $\alpha : Q(F) \to Q_2$ defined by

$$\alpha(p) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \in P \\ -1 & \text{if } a \in -P \end{cases}$$

is a hyperring homomorphism. This is clear. Conversely, if $\alpha : Q(F) \to Q_2$ is a hyperring homomorphism then $P := \{a \in F : \alpha(a) = 1\}$ is an ordering. This is clear. The fact that $P \leftrightarrow \alpha$ defines a bijection is also clear.

Corollary 6.2. Suppose $F_1 \sim F_2$. Then orderings on $F_1$ are in one-to-one correspondence with orderings on $F_2$.

Proof. this is clear.

We give an example to show how Corollary 6.2 can fail when orderings are replaced by valuations.

Example 6.3. Let $F = k((t))$, where $k$ is an algebraically closed field, char $k \neq 2$. Denote by $v$ the natural valuation on $F$, i.e.,

$$v(\sum_{i=k}^{\infty} a_i t^i) := \min\{i : a_i \neq 0\} \text{ if } \sum_{i=k}^{\infty} a_i t^i \neq 0.$$

The residue field of $(F, v)$ is $k$, the value group is $\mathbb{Z}$. Applying Theorem 4.1, we see that $Q(F)$ is a group extension of $Q(k) = \{0, 1\}$ by a cyclic group of order 2, so $Q(F) = \{0, 1, p\}$, $p \in Q(F) \setminus Q(k)$, $a + 0 = a$, $1 + 1 = p + p = \{0, 1, p\}$, $1 + p = \{1, p\}$, $a \cdot 0 = 0$, $1 \cdot 1 = p$, $p \cdot p = 1$, $1 \cdot p = p$. Thus we see that $Q(F) \cong Q(\mathbb{F}_5)$, so $F \sim \mathbb{F}_5$. At
the same time, \( F \) has lots of non-trivial valuations, whereas \( \mathbb{F}_5 \) has only the trivial valuation.

If \( i : F_1 \hookrightarrow F_2 \) is an embedding of fields of characteristic \( \neq 2 \), then \( i(F_1^{*2}) \subseteq F_2^{*2} \), so \( i \) induces a hyperfield homomorphism \( Q(i) : Q(F_1) \to Q(F_2) \) defined by \( Q(i)(\overline{a}) = \overline{i(a)} \). In this way, \( Q \) can be viewed as a functor.

**Example 6.4.**

(i) Let \( F_p \) denote the real closure of the ordered field \((F, P)\). The field embedding \( F \hookrightarrow F_p \) induces a hyperring homomorphism \( Q(F) \to Q(F_p) \). This factors through the quotient hyperfield \( F/\mathbb{m}P \) and \( Q(F_p) \cong F/\mathbb{m}P \cong \mathbb{Q}_2 \). This provides another way of understanding Theorem 6.1.

(ii) Denote by \( \tilde{F}_v \) the Henselization of the valued field \((F, v)\). The embedding \( F \hookrightarrow \tilde{F}_v \) induces a hyperring homomorphism \( Q(F) \to Q(\tilde{F}_v) \). In the non-dyadic case, \( Q(F) \to Q(\tilde{F}_v) \) factors through the quotient hyperfield \( F/\mathbb{m}(1 + M_v)F^{*2} \) and \( Q(\tilde{F}_v) \cong F/\mathbb{m}(1 + M_v)F^{*2} \).

We need some terminology.

**Definition 6.5.** Let \( T \) be a subgroup of \( F^{*} \).

(i) We say \( x \in F^{*} \) is \( T \)-rigid if \( T + Tx \subseteq T \cup Tx \).

(ii) \( B(T) := \{x \in F^{*} : \text{ either } x \text{ or } -x \text{ is not } T \text{-rigid} \} \).

(iii) Elements of \( B(T) \) are said to be \( T \)-basic.

Note: (i) If \( x \in F^{*} \) is \( T \)-rigid and \( y = tx, t \in T \), then \( y \) is \( T \)-rigid. (ii) Consequently, \( B(T) \) is a union of cosets of \( T \). (iii) \(-1\) is not \( T \)-rigid (because \( 0 \in T - T \)), so \( \pm T \subseteq B(T) \).

**Definition 6.6.** Let \( T \) be a subgroup of \( F^{*} \). We say that \( T \) is exceptional if \( B(T) = \pm T \) and either \(-1 \in T \) or \( T \) is additively closed.

**Theorem 6.7.** Let \( T \subseteq F^{*} \) be a subgroup and \( H \subseteq F^{*} \) be a subgroup containing \( B(T) \). Then there exists a subgroup \( \overline{H} \) of \( F^{*} \) such that \( H \subseteq \overline{H} \) and \( (\overline{H} : H) \leq 2 \) and a valuation \( v \) of \( F \) such that \( 1 + M_v \subseteq T \) and \( U_vT \subseteq \overline{H} \). Moreover, \( \overline{H} = H \) works, unless \( T \) is exceptional.

**Proof.** Omitted.


In Theorem 6.7 there is no assumption that \( F^{*2} \subseteq T \), although in our applications to Witt equivalence we will always be assuming this.

There is no known analog of Theorem 6.7 in the dyadic case. This is an open problem. See B. Jacob, R. Ware 1991 for a partial analog.

### 7. Global fields

**Definition 7.1.** A function field in one variable over a field \( k \) is an extension field \( F \) of \( k \) which is finitely generated over \( k \) and has transcendence degree 1 over \( k \).

**Definition 7.2.** A global field is a number field (i.e., a finite extension of \( \mathbb{Q} \)) or function field in one variable over a finite field. The finite primes of a global field are the discrete rank one valuations. In the function field case these are the only primes. In the number field case there are also infinite primes which are field embeddings into \( \mathbb{R} \) or conjugate pairs of field embeddings into \( \mathbb{C} \).
Let \( p \) be a prime of a global field \( F \). We denote by \( \hat{F}_p \) the completion of \( F \) at \( p \). If \( p \) is a valuation this is a local field. If \( p \) is an infinite prime it is \( \mathbb{R} \) or \( \mathbb{C} \).

**Theorem 7.3.** Let \( E, F \) be global fields of characteristic \( \neq 2 \). Then \( E \sim F \) iff there exists a one-to-one correspondence between primes of \( E \) and primes of \( F \) (including infinite primes, if any) such that if \( p \leftrightarrow q \) then \( \hat{E}_p \sim \hat{F}_q \).

**Proof.** Omitted. \( \square \)

For real infinite primes (if any), the correspondence is defined using Corollary 6.2. For nondyadic finite primes the correspondence is defined using Theorem 6.7. For complex infinite primes (if any) and dyadic finite primes (if any), a different argument is needed. See R. Perlis, K. Szymiczek, P.E. Conner, R. Litherland 1994 for the proof of Theorem 7.3.

Setting up the one-to-one correspondence in Theorem 7.3 is usually referred to as “matching Witts” because in the English language this provides an amusing play on words.

There is also the following useful addendum to Theorem 7.3, due to J. Carpenter 1992.

**Theorem 7.4.** Let \( E, F \) be global fields of characteristic \( \neq 2 \). Then \( E \sim F \) iff

(A) \(-1 \in E^{*} \) iff \(-1 \in F^{*} \),

(B) \( E \) and \( F \) have the same number of real infinite primes, and

(C) there is a bijection between dyadic finite primes of \( E \) and dyadic finite primes of \( F \) such that if \( p \leftrightarrow q \) then \([\hat{E}_p : \mathbb{Q}_2] = [\hat{F}_q : \mathbb{Q}_2] \) and \(-1 \in \hat{E}_p \) iff \(-1 \in \hat{F}_q \).

**Proof.** Omitted. \( \square \)

### 8. Function fields in one variable

**Definition 8.1.** Let \( F \) be a function field in one variable over a field \( k \). The field of constants of \( F \) over \( k \) is defined to be the relative algebraic closure of \( k \) in \( F \).

One knows in the set-up of Definition 8.1 that the field of constants of \( F \) over \( k \) is a finite extension of \( k \).

Throughout this section, we assume that \( F \) is a function field in one variable over a field \( k \), char \( k \neq 2 \). We consider various cases:

(i) We have considered already, in the previous section, the case where \( k \) is a finite field. In this case \( F \) is a global field with no infinite primes and no dyadic primes, so the Witt equivalence class of \( F \) depends only on whether \( \sqrt{-1} \in F \) or \( \sqrt{-1} \notin F \); see Theorem 7.4. Note that, since \( \sqrt{-1} \) is algebraic over \( k \), \( \sqrt{-1} \in F \) iff \( \sqrt{-1} \in k' \), where \( k' \) denotes the field of constants of the extension \( F \) of \( k \). Note also that since \( k \) is finite \( k' \) is also finite. Consequently, the Witt equivalence class of \( F \) depends only on whether \( |k'| \equiv 1 \) or \( 3 \mod 4 \).

(ii) Suppose now that \( k \) is algebraically closed. Then \( F \) is a \( C_1 \) field, so every quadratic form in 3 or more variables has a non-trivial zero, by an old result of C. Tsen 1933. This implies that, for any \( a, b \in Q(F)^{*} \), \( a + b = Q(F) \) if \( b = -a \) and \( a + b = Q(F)^{*} \) if \( b \neq -a \). Also, \( -a = a \) (because \( -1 \) is a square in \( k \)). At the same time, it is possible to show that the group structure of \( Q(F)^{*} \) depends only on the cardinality of \( k \). Consequently, one has the following:

**Theorem 8.2.** Suppose \( F_i \) is an algebraic function field in one variable over an algebraically closed field \( k_i \), char \( k_i \neq 2 \), \( i = 1, 2 \). Then \( F_1 \sim F_2 \) iff \( |k_1| = |k_2| \).
(iii) Suppose now that \( k \) is real closed. The following result is proved by P. Koprowski 2002 and N. Grenier-Boley, D.W. Hoffmann (with appendix by C. Scheiderer) 2013:

**Theorem 8.3.** Let \( F \) be an algebraic function field in one variable over \( k \), i.e., a finite extension of the rational function field \( k(t) \), where \( k \) is a real closed field. Then

\[
F \sim \begin{cases} 
  k(t) & \text{if } F \text{ has at least one ordering} \\
  k(t)(\sqrt{-1}) & \text{if } \sqrt{-1} \in F \\
  k(t)(\sqrt{-1}(t^2 + 1)) & \text{otherwise}
\end{cases}
\]

Note that, in Theorem 8.3, the fact that \( \sqrt{-1} \in F \Rightarrow F \sim k(t)(\sqrt{-1}) \) is already a consequence of Theorem 8.2.

(iv) For algebraic functions in one variable over a general field \( k \) of characteristic \( \neq 2 \), results are somewhat less conclusive; see P. Koprowski 2002.