HERMITIAN FORMS

HAROLD COOPER

1. Quadratic Extension Fields

Definition 1.1. If δ satisfies some irreducible quadratic equation in a field F, then $F(\delta)$ is a *quadratic extension field* of F.

We can make up lots of quadratic extension fields for any field just by considering the square root of any non-square element of the field. For example, $\mathbb{F}_5(\sqrt{2})$ is the extension of $\mathbb{F}_5$ with the relation $(\sqrt{2})^2 = 2$.

But of course the primary example of a quadratic extension field is the complex numbers which extend the reals as $\mathbb{C} = \mathbb{R}(i)$ where $i^2 + 1 = 0$.

One of the may cool things one can do in the complex numbers is complex conjugation. An obvious question is whether there is an analogous operation on *any* quadratic extension field, and the answer is yes; for since every element of a quadratic extension $F(\delta)$ is of the form $a + b\delta$ for $a, b \in \mathbb{F}$, we can define the automorphism $\phi(a + b\delta) = a - b\delta$ perhaps more concisely written as $\overline{a + b\delta} = a - b\delta$.

Note that this automorphism has $\phi \neq 1$ but $\phi^2 = 1$, i.e. it has order 2 in the group of automorphisms on $F(\delta)$. Note furthermore that every element of $a \in F \subset F(\delta)$ is fixed by ϕ since $\overline{a} = \overline{a + 0\delta} = a - 0\delta = a$, and no element of $F(\delta)\backslash F$ is fixed since for $b \neq 0$, $\overline{a + b\delta} = a - b\delta \neq a + b\delta$ (and yes, as usual, we are assuming $\operatorname{char} F \neq 2$).

We are interested in what ϕ fixes since it allows us to work with a field even if we're not sure that it's a quadratic extension field: all we need is an automorphism ϕ of order 2 and then the subfield fixed by ϕ can be thought of as our F, and α can then be any element of our field but not in F.

2. Hermitian Forms

In the a complex vector space $\mathbb{C}^n$, the most useful inner product is defined for vectors $u = \begin{pmatrix} u_1 & \dots & u_n \end{pmatrix}$ and $v = \begin{pmatrix} v_1 & \dots v_n \end{pmatrix}$ as $\langle u, v \rangle = \sum_i u_i \overline{v_i}$, since this reduces to $\|v\|^2 = \langle v, v \rangle = \sum_i |v_i|^2$ for $u = v$. We generalized the concept of conjugates; can we generalize this type of inner product as well?

Again, yes we can. The fundamental properties are that:

(1) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
(2) $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$
(3) $\langle au, v \rangle = a \langle u, v \rangle = \langle u, \overline{a} v \rangle$ for any a in the extension field
(4) $\langle u, v \rangle = \overline{\langle v, u \rangle}$

Definition 2.1. A form with the first three properties is *sesquilinear* and a form with all four properties is *Hermitian.*

Thus sesquilinear forms (which include the Hermitian forms, if that wasn't clear) are *almost* bilinear, differing only in their treatment of scalar multiples of their second arguments (the second half of (3), above). Furthermore, you may note that (4) above makes Hermitian forms have similar properties to symmetric forms, as seen in the following proposition. Note that at this point we assume throughout these notes that F is a field with an automorphism ϕ of order 2 where we denote $\overline{a} \stackrel{\text{def}}{=} \phi(a)$, V is a vector space over F, and $B\colon V \times V \to F$ is a form on V.

Definition 2.2. A matrix A is *Hermitian* when $A = \overline{A^t}$ (where by conjugation of a matrix we mean simply conjugation of each of its elements).

Thus note that the Hermitian matrices in the subspace of vectors with entries only in the fixed field of conjugation (e.g. $\mathbb{R}$ in the case of $\mathbb{C}$) are exactly the symmetric matrices in that subspace.

Proposition 2.1. *If $\hat{B}$ is a matrix for B under some basis then B is Hermitian iff $\hat{B}$ is Hermitian.*

As a final generalization of our use of conjugation in $\mathbb{C}$, we define an analogue to the vector norm in $\mathbb{C}^n$, i.e. we associate a quadratic form $Q\colon V \to F$ with B by $Q(v) = B(v, v)$.

Proposition 2.2. *If B is nonzero and Hermitian then Q is nonzero.*