

117 - SS2 - MP2 - August 6th, 2021

[2] A bilinear form  $\omega$  on  $V \oplus V$  for  $\mathbb{F}$ -vector space is symmetric if  $\omega(x, y) = \omega(y, x)$  for all  $x, y \in V$ . A quadratic form on  $V$  is a function  $q : V \rightarrow \mathbb{F}$  obtained from a bilinear form  $\omega$  by writing  $q(x) = \omega(x, x)$ .

- (a) Prove that if  $\text{char}(\mathbb{F}) \neq 2$  then every symmetric bilinear form is uniquely determined by the corresponding quadratic form.

*Proof.* Let  $\omega$  be a symmetric bilinear form in a vector space  $V$ , we will show that  $\omega(x) = (x, x)$  is a quadratic form in the same vector space  $V$ . We see first that

$$\omega(\alpha x) = (\alpha x, \alpha x) = \alpha^2(x, x) = \alpha^2\omega(x).$$

Now we must show  $b_\omega(x, y) = \omega(x + y) - \omega(x) - \omega(y)$  is a symmetric bilinear form. We can see that this is satisfied by the following,

$$\begin{aligned} b_\omega(x, y) &= \omega(x + y) - \omega(x) - \omega(y) \\ &= (x + y, x + y) - (x, x) - (y, y) \\ &= (x, x + y) + (y, x + y) - (x, x) - (y, y) \\ &= (x, x) + (x, y) + (y, x) + (y, y) - (x, x) - (y, y) \\ &= (x, y) + (y, x) && \omega \text{ is a symmetric bilinear form so,} \\ &= 2(x, y) \end{aligned}$$

Recall though that  $\omega$  was defined as a symmetric bilinear form, therefore  $b_\omega$  is a symmetric bilinear form.

Now for the converse, let  $\omega(x) = (x, x)$  be a quadratic function,

$$\begin{aligned} b_\omega(x, x) &= \omega(x + x) - \omega(x) - \omega(x) \\ &= (x + x, x + x) - (x, x) - (x, x) \\ &= 4(x, x) - 2(x, x) \\ &= 2(x, x) \end{aligned}$$

$$\frac{1}{2}b_\omega(x) = (x, x)$$

□

Thus we see  $\frac{1}{2}b_\omega(x, x)$  is the bilinear form determined by the quadratic form  $\omega(x) = (x, x)$

- (b) Is the conclusion of part (a) still true if  $\text{char}(\mathbb{F}) = 2$ ?

**Answer:** No. As we see at the end if the characteristic of the underlying field were to be 2 that would mean 2 would not exist in the field and we wouldn't be able to divide by 2.

- (c) Yes. The quadratic forms have a 1-1 correspondence with symmetric bilinear forms, but non symmetric bilinear forms can define the same quadratic form as some symmetric bilinear form. This is because every bilinear form  $\omega$  gives a quadratic form by  $q(x) = \omega(x, x)$ , but we see it doesn't concern the antisymmetric form of  $\omega$ , therefore not effecting  $q$ . This is why you can have a non symmetric bilinear form and a symmetric bilinear form define the same quadratic form.

[1] For all the following make the application of the Axiom of Choice (or any equivalent statement) explicit in the argument.

- (a) Prove that every vector space has a basis.

*Proof.* We know from class that if  $V$  is a finite dimensional vector space we can consider the set  $X_1$  containing a single non-zero vector of  $x \in V$ . if  $X$  spans the whole vector space then we are done. If not we can take another vector  $x \in V$  and not in the span of  $X_1$ . We can define the set  $X_2 = X_1 \cup \{x\}$  and if this doesn't span the whole vector space we can repeat the process until it terminates. The issues that arises isn't with finite dimensional vector spaces but for infinite ones.

To prove that infinite dimensional vector spaces do indeed have a basis let us consider the collection  $S$  which is a collection of subsets of some set. Also that whenever these subsets form a chain such that  $S_1 \subset S_2 \subset S_3 \dots$  that the union of these subsets is in  $S$ . Applying Zorn's Lemma which is an equivalent statement to the Axiom of Choice, we know there exists a maximal element in  $S$  such that it is not properly contained by other elements in  $S$ , which implies every element in  $S$  is contained in this maximal element in  $S$ .

We can now let this collection  $S$  be the collection of all linearly independent subsets of  $V$ . Because the union of an increasing chain of linearly independent sets is also a linearly independent set, we can apply Zorn's Lemma as stated before and guarantee that there will be a maximal linearly independent set in this collection. This maximal linearly independent set will then serve as the basis for  $V$ . The reason we know it can is if there were to exist another linearly independent vector in  $V$  not covered by the span of the maximal set, then that would be a contradiction since the maximal set by definition cannot be properly contained by another subset.  $\square$

- (b) Let  $\dim_{\mathbb{F}}(V)$  denote the dimension of the vector space  $V$  over the field  $\mathbb{F}$ . What is  $\dim_{\mathbb{R}}(\mathbb{R}^2)$ ? How about  $\dim_{\mathbb{Q}}(\mathbb{R}^2)$

*Proof.* We know from the class and the textbook that the dimension of a finite dimensional vector space over a field  $\mathbb{F}$  is simply the number of elements in the basis of said vector space. So in the case of the  $\mathbb{R}$ -vector space  $\mathbb{R}^2$  we know it's basis is the following

$$\{(1, 0), (0, 1)\}$$

We know the span of this set covers the whole vector space because any vector in  $\mathbb{R}^2$  can be expressed as the following,

$$(x, y) = a(1, 0) + b(0, 1)$$

Where  $a = x$ , and  $b = y$ . We know we can do this since  $x, y \in \mathbb{R}$  and since  $\mathbb{R}^2$  is over the field  $\mathbb{R}$ ,  $a, b \in \mathbb{R}$

For  $\dim_{\mathbb{Q}}(\mathbb{R}^2)$  we know because of the axiom of choice a basis exists for an infinite dimensional vector space. We also know  $\dim_{\mathbb{R}}(\mathbb{R}[x]) = |\mathbb{N}|$ . Meaning it is countably infinite, thus  $\dim_{\mathbb{Q}}(\mathbb{R}^2)$  is uncountably infinite. We can get an idea of what this basis is by trying to construct it. Imagine we have the form like before,

$$(x, y) = a(1, 0) + b(0, 1)$$

Say  $x$  is  $\sqrt{2}$ . We know this is irrational and therefore exists outside of  $\mathbb{Q}$ . If we add it as a vector we can repeat the process for  $\sqrt{3}$  and repeat forever using our favorite irrational numbers. The uncountably infinite parts comes in because we know from real analysis there are far more irrational numbers than there are rational numbers which is why the reals are uncountably infinite and the rationals countably infinite. So the basis will look like a set of infinitely linearly independent vectors that are composed of values in  $\mathbb{R}$   $\square$

(c) Am stuck on this and ran out of time.....