Dartmouth College Department of Mathematics
Math 101 Topics in Algebra: Quadratic Forms
Fall 2020

Problem Set # 1 (due Monday October 19)

Problems:

1. Write down a bilinear form whose left and right kernels are not equal. Write down a nondegenerate bilinear form that is neither symmetric nor skew-symmetric such that the left and right kernels are equal.

2. Let V and W be finite dimensional F-vector spaces.

(a) Prove that $\dim_F(V \otimes W) = \dim_F V \cdot \dim_F W$.

(b) If $\boldsymbol{x} = \{x_1, \dots, x_n\}$ and $\boldsymbol{y} = \{y_1, \dots, y_m\}$ are bases for V and W, respectively, prove that $\boldsymbol{x} \otimes \boldsymbol{y} = \{x_i \otimes y_j \mid 1 \le i \le n,\ 1 \le j \le m\}$ is a basis for $V \otimes W$.

(c) For vectors $v_1, v_2 \in V$, we write $v_1\, v_2$ for the coset of $v_1 \otimes v_2$ in $S^2 V$. If $\boldsymbol{x} = \{x_1, \dots, x_n\}$ is a basis for V, prove that $S^2\boldsymbol{x} = \{x_i\, x_j \mid 1 \le i \le j \le n\}$ is a basis for $S^2 V$.

(d) For vectors $v_1, v_2 \in V$, we write $v_1 \wedge v_2$ for the coset of $v_1 \otimes v_2$ in $\bigwedge^2 V$. If $\boldsymbol{x} = \{x_1, \dots, x_n\}$ is a basis for V, prove that $\wedge^2\boldsymbol{x} = \{x_i \wedge x_j \mid 1 \le i < j \le n\}$ is a basis for $\bigwedge^2 V$.

(e) Prove that the map $V^\vee \otimes W \to \mathrm{Hom}_F(V, W)$ defined by $f \otimes w \mapsto \big(u \mapsto f(u)w\big)$ is an isomorphism is F-vector spaces.

(f) Prove that the map $V^\vee \otimes W^\vee \to (V \otimes W)^\vee$ defined by $f \otimes g \mapsto \big(v \otimes w \mapsto f(v)g(w)\big)$ is an isomorphism of F-vector spaces.

(g) Prove that the map $\bigwedge^2(V^\vee) \to \big(\bigwedge^2 V\big)^\vee$ defined by $f \wedge g \mapsto \big(v \wedge w \mapsto f(v)g(w) - f(w)g(v)\big)$ is an isomorphism of F-vector spaces.

(h) Prove that the map $S^2(V^\vee) \to \big(S_2 V\big)^\vee$ defined by $f\, g \mapsto \big(v \otimes v \mapsto f(v)g(v)\big)$ is an isomorphism of F-vector spaces.

(i) Prove that the map $V \otimes W \to W \otimes V$ defined by $v \otimes w \mapsto w \otimes v$ is an isomorphism of F-vector spaces.

For all these maps, you should understand (if not explain), why they can even be defined as they are.

3. Let $f : V \to W$ be an F-linear map between finite dimensional F-vector spaces and let $\boldsymbol{x} = \{x_1, \dots, x_n\}$ and $\boldsymbol{y} = \{y_1, \dots, y_m\}$ be bases for V and W, respectively. Let M be the matrix representing f with respect to the bases $\boldsymbol{x}$ and $\boldsymbol{y}$.

(a) Consider the F-linear map $f \otimes f : V \otimes V \to W \otimes W$ defined by $v_1 \otimes v_2 \mapsto f(v_1) \otimes f(v_2)$ and describe the matrix representing $f \otimes f$ with respect to the bases $\boldsymbol{x} \otimes \boldsymbol{x}$ and $\boldsymbol{y} \otimes \boldsymbol{y}$ in terms of the matrix M.

(b) Prove that $f \otimes f$ induces an the F-linear map $S^2 f : S^2 V \to S^2 W$ and describe the matrix representing $S^2 f$ with respect to the bases $S^2\boldsymbol{x}$ and $S^2\boldsymbol{y}$ in terms of the matrix M.

(c) Prove that $f \otimes f$ induces an the F-linear map $\bigwedge^2 f : \bigwedge^2 V \to \bigwedge^2 W$ and describe the matrix representing $\bigwedge^2 f$ with respect to the bases $\wedge^2\boldsymbol{x}$ and $\wedge^2\boldsymbol{y}$ in terms of the matrix M.

4. Let (V, q) be a quadratic form, $v \in V$ such that $q(v) \neq 0$, and $r_v : V \to V$ the reflection defined by $r_v(w) = w - \frac{b_q(v,w)}{q(v)} v$.

(a) Prove that $r_v \in O(q)$.

(b) Assume that q is nondegenerate and $\mathrm{char}(F) \neq 2$. Prove that if $w \in V$ satisfies $q(v) = q(w)$, then there exists a reflection r such that $r(v) = \pm w$. **Hint.** Reflect through $v \pm w$.

5. *Characteristic 2, scary!* Let F be a field of characteristic 2 and $a, b \in F$. Define the quadratic form $[a, b]$ on F^2 by $(x, y) \mapsto ax^2 + xy + by^2$. Let h be the hyperbolic form on F^2 defined by $(x, y) \mapsto xy$.

(a) Prove that if a binary quadratic form q over F has a nondegenerate associated bilinear form b_q, then q is isometric to $[a, b]$ for some $a, b \in F$.

(b) Prove that $h \cong [0, 0] \cong [0, a]$ for any $a \in F$.

(c) Let $\wp : F \to F$ be the Artin–Schreier map $x \mapsto x^2 + x$. For $a \in F$ prove that $[1, a]$ is isotropic if and only if $a \in \wp(F)$. As an example, prove that over $F = \mathbb{F}_2(t)$ the quadratic form $x^2 + xy + ty^2$ is anisotropic. **Note.** The group $F/\wp(F)$ plays the role of the group of square classes.

(d) Prove that if q is a quadratic form over F with b_q is nondegenerate then q can be written as an orthogonal sum $\perp_{i=1}^{m} [a_i, b_i]$. This is "diagonalization" in characteristic 2.

6. Let F be an arbitrary field. Consider the hyperbolic quadratic form $h(x, y) = xy$ on F^2 and it's associated symmetric bilinear form $b((x, y), (x', y')) = xy' + x'y$. Also consider the alternating bilinear form $a((x, y), (x', y')) = xy' - x'y$ on F^2. The group of isometries of an alternating bilinear form a is called the *symplectic group* of a and is denoted $\mathrm{Sp}(a)$.

(a) Prove that $\mathrm{O}(h)$ is isomorphic to the semi-direct product $F^\times \rtimes C_2$, where C_2 is a group of order 2.

(b) Prove that $\mathrm{Sp}(a) = \mathrm{SL}_2(F)$, the group of 2×2 matrices of determinant 1 over F.

(c) Prove that if F has characteristic $\neq 2$, then $\mathrm{O}(b) = \mathrm{O}(h)$. **Hint.** A proof of a more general result was indicated in lecture.

(d) Prove that if F has characteristic 2, then $\mathrm{O}(b) = \mathrm{Sp}(a)$.

So really, in characteristic 2, we should think of the associated bilinear form as an alternating form and not a symmetric form, since it's orthogonal group is actually a symplectic group!

7. *Subgroups of fields.* You only need to work on this problem if you have not solved a similar one before in your life (but please let me know this). Let F be a field.

(a) Let G be a finite abelian group. Prove that G is cyclic if and only if G has at most m elements of order dividing m for each $m \mid \#G$. **Hint.** You'll need the structure theorem of finite abelian groups?

(b) Prove that every finite subgroup G of the multiplicative group $F^\times = F \smallsetminus \{0\}$ is cyclic. **Hint.** You'll need to use the fact that a polynomial of degree m has at most m roots in F, which you can prove using the division algorithm for polynomials.

(c) Deduce that if F is a finite field then $F^\times$ is cyclic. For each field F having at most 7 elements, find an explicit generator of $F^\times$.

(d) Prove that for any finite field of odd characteristic $F^\times/F^{\times 2}$ is a group of order 2.