Finite Geomtry and Geometric Algebra

Semester Project Report
January Semester, 2025

Dinesh Karthik Mulumudi
Third Year BS-MS Student
Roll no. 20221165

Supervisor: Prof. Krishna Kaipa

Preface

This report presents the compilation of my semester project investigating advanced topics in algebra and geometry and coding theory, with particular emphasis on reflexive forms, bilinear forms, symplectic groups, and their applications in finite geometry.

Initially motivated by an interest to explore theoretical computer science, the project evolved into a reading-focused study with a stronger algebraic orientation. The report is structured in two chapters: the first concentrates on classifying σ-sesquilinear and reflexive forms, alternating and quadratic forms, adopting a linear algebra perspective; the second employs a group-theoretic approach to explore projective spaces, transvections in generating special linear groups, and the geometric structure of symplectic groups.

Later sections provide concise refreshers on finite fields, group actions, and quotient topology—foundational tools for understanding the key concepts discussed. I've also included a brief overview of coding theory with several notable results, inspired by Prof. Krishna Kaipa's talk "What is Coding Theory?". Where relevant, I've incorporated alternative proofs shared during our discussions. The report concludes with a comprehensive bibliography of references that contributed significantly to this study.

I extend my sincere gratitude to my Supervisor **Prof. Krishna Kaipa**, and my peers, Meghana and Vijay Patidhar, for their guidance and enlightening discussions that substantially enriched this work. I hope this report serves as a valuable resource for those interested in the elegant interplay between algebra, geometry, and coding theory.

Dinesh Karthik M
20221165
Third Year BS-MS Student
IISER Pune

Contents

Chapter 1

Forms

The main aim of this chapter is to classify all reflexive σ-sesquilinear forms and quadratic forms defined on a finite-dimensional vector space over a finite field.

1.1 σ-Sesquilinear Forms

Definition 1.1.1. Let $V_k(F)$ denote the k-dimensional vector space over the field F. Let σ be an automorphism of F. A σ-sesquilinear form is a map from $V_k(F) \times V_k(F)$ to F such that:

- $b(u, v)$ is linear in u for fixed $v \in V_k(F)$.
- $b(u, v)$ is additive in v for fixed $u \in V_k(F)$.
- $b(u, \lambda v) = \lambda^\sigma b(u, v)$ for all $v \in V_k(F)$ and $\lambda \in F$.

Thus, if σ is the identity automorphism, then a σ-sesquilinear form is simply a bilinear form.

Definition 1.1.2. Two σ-sesquilinear forms b and b' are isometric (or equivalent) if there exists an isomorphism α of $V_k(F)$ such that

$$b(u, v) = b'(\alpha(u), \alpha(v))$$

for all $u, v \in V_k(F)$.

Definition 1.1.3. A σ-sesquilinear form is degenerate if there exists a nonzero vector $u \in V_k(F)$ such that

$$b(u, v) = 0 \quad \text{for all } v \in V_k(F).$$

Definition 1.1.4. Let b be a σ-sesquilinear form. For any subset U of $V_k(F)$, define its orthogonal subspace as

$$U^\perp = \{v \in V_k(F) \mid b(u, v) = 0 \text{ for all } u \in U\}.$$

Definition 1.1.5. A vector u is isotropic if $b(u, u) = 0$. A subspace U is totally isotropic if

$$b(u, v) = 0 \quad \text{for all } u, v \in U.$$

A maximum totally isotropic subspace is a totally isotropic subspace that is not contained in any larger totally isotropic subspace.

Definition 1.1.6. A hyperbolic subspace with respect to b is a two-dimensional subspace $\langle u, v\rangle$ where

$$b(u,u) = 0, \quad b(v,v) = 0, \quad \text{and} \quad b(u,v) \neq 0.$$

Lemma 3.1. Let U be a subspace of $V_k(F)$. If b is a non-degenerate σ-sesquilinear form on $V_k(F)$, then

$$\dim U + \dim U^{\perp} = k.$$

Lemma 3.2. For subspaces U and U' of $V_k(F)$,

$$U^{\perp} \cap U'^{\perp} = (U + U')^{\perp}.$$

Theorem 3.3. A totally isotropic subspace U, with respect to a non-degenerate σ-sesquilinear form, satisfies:

$$\dim U \leq \left\lfloor \frac{k}{2} \right\rfloor.$$

1.2 Classification of Reflexive Forms

Definition 1.2.1. A σ-sesquilinear form b is reflexive if

$$b(u,v) = 0 \implies b(v,u) = 0.$$

Theorem 1.2.2. *A totally isotropic subspace, with respect to a non-degenerate σ-sesquilinear form on $V_k(F)$, has dimension at most $\lfloor k/2 \rfloor$.*

Theorem 1.2.3. *A non-degenerate reflexive σ-sesquilinear form on $V_k(F)$ is, up to scalar factor, one of the following types:*

1. *Alternating form: $b(u,u) = 0$ for all $u \in V_k(F)$.*
2. *Symmetric form: $b(u,v) = b(v,u)$ for all $u, v \in V_k(F)$.*
3. *Hermitian form: $b(u,v) = b(v,u)^{\sigma}$ for all $u, v \in V_k(F)$, where $\sigma^2 = id$ and $\sigma \neq id$.*

1.3 Alternating Forms

Let F be an arbitrary field and let V be a n dimensional vector space over F. We assume familiarity with the vector spaces

1. V^* (the dual vector space)
2. $\otimes^r V$ (the r-th tensor power of V)
3. $\mathrm{Sym}^r(V)$ (the r-th symmetric power of V)
4. $\wedge^r V$ (the r-th exterior power of V).

For example Section 11.5 of Dummit-Foote. If $e_1, \ldots, e_n$ is any basis of V, there are corresponding *associated bases* for these vector spaces:

1. the dual basis $e^1, \ldots, e^n$ for V^* defined by $e^i(e_j) = \delta_{ij}$,

2. the n^r basis elements $e_{i_1} \otimes \cdots \otimes e_{i_r}$ for any sequence $(i_1, \ldots, i_r)$ with each $i_s \in \{1, \ldots, n\}$

3. the $\binom{n+r-1}{r}$ basis elements $e_{i_1} \ldots e_{i_r}$ for any non-decreasing sequence $(i_1, \ldots, i_r)$ with each $i_s \in \{1, \ldots, n\}$.

4. the $\binom{n}{r}$ basis elements $e_{i_1} \wedge \cdots \wedge e_{i_r}$ for any increasing sequence $(i_1, \ldots, i_r)$ with each $i_s \in \{1, \ldots, n\}$. We note that $\wedge^n V$ is one-dimensional.

If $T : V \to W$ is a linear map, then we have associated maps $T^* : W^* \to V^*$, and maps $\otimes^r T : \otimes^r V \to \otimes^r W$, $\mathrm{Sym}^r T : \mathrm{Sym}^r(V) \to \mathrm{Sym}^r(W)$ and $\wedge^r T : \wedge^r(V) \to \wedge^r(W)$. For example, if $V = F^n$ and $T \in M_n(F)$, then $\wedge^n T = \det(T)$.

It is useful to know not just these vector spaces, but also the algebra structure on $\otimes V = \oplus_{r \geq 0} \otimes^r V$, $\mathrm{Sym}(V) = \oplus_{r \geq 0} \mathrm{Sym}^r V$ and $\wedge V = \oplus_{r \geq 0} \wedge^r V$. For example, the algebra $\mathrm{Sym}(V^*)$ is very familiar to us: it is the algebra of polynomials in n indeterminates $X_1, \ldots, X_n$ with entries in the field F (where we think of X_i as e^i).

1.3.1 Canonical form of an alternating matrix

Let A be an $n \times n$ alternating matrix with entries in F. Recall this means that $A_{ii} = 0$ and $A_{ij} = -A_{ji}$.

Lemma 1.3.1. *There is a canonical isomorphism $(\wedge^r(V))^* \simeq \wedge^r(V^*)$. This isomorphism has the property that if $e_1, \ldots, e_n$ is any basis of V, then the basis of $(\wedge^r(V))^*$ dual to the basis $\{e_{i_1} \wedge \cdots \wedge e_{i_r} : (i_1, \ldots, i_r) \textit{increasing}\}$ maps to the basis $\{e^{i_1} \wedge \cdots \wedge e^{i_r} : (i_1, \ldots, i_r) \textit{increasing}\}$ (more precisely we mean that the basic vector dual to $e_{i_1} \wedge \cdots \wedge e_{i_r}$ maps to the basic vector $e^{i_1} \wedge \cdots \wedge e^{i_r}$)*

Proof. Given $(v_1, \ldots, v_r) \in V \times \cdots \times V$ and $(f_1, \ldots, f_r) \in V^* \times \cdots \times V^*$, we note that the determinant of the $r \times r$ matrix whose (ij)-th entry is $f_i(v_j)$ is alternating and multilinear in both $(v_1, \ldots, v_r)$ as well as $(f_1, \ldots, f_r)$ and hence gives (by the universal property of exterior power spaces) a bilinear map

$$\wedge^r(V) \otimes \wedge^r(V^*) \to F.$$

If $e_1, \ldots, e_n$ is a basis of V and the associated bases of $\wedge^r(V)$ and $\wedge^r(V^*)$ are as above, then the matrix of this bilinear map wrt the associated bases is just the identity matrix (of size $\binom{n}{r}$). Thus, this bilinear map gives the desired isomorphism between $(\wedge^r(V))^*$ and $\wedge^r(V^*)$. Under this isomorphism we have shown above that basic vector of $(\wedge^r(V))^*$ dual to the basic vector $e_{i_1} \wedge \cdots \wedge e_{i_r}$ of $\wedge^r V$ maps to $e^{i_1} \wedge \cdots \wedge e^{i_r}$ □

An alternating bilinear form $b : V \times V \to F$ is simply an element of $(\wedge^2 V)^*$. Thus, by lemma above, we may think of alternating bilinear forms of elements of $\wedge^2(V^*)$. In particular, if B is the $n \times n$ alternating matrix representing the alternating bilinear form b, wrt a basis $e_1, \ldots, e_n$ of V, then the corresponding element $\Omega_b \in \wedge^2(V^*)$ has the expression

$$\Omega_b = \sum_{i<j} B_{ij} e^i \wedge e^j.$$

Theorem 1.3.2. *Let b be an alternating bilinear form on a n dimensional vector space V over an arbitrary field F. There is a basis $e_1, \ldots, e_n$ of V wrt which the matrix of b is of the form*

$$B = \begin{pmatrix} A_{2r\times 2r} & 0_{2r\times n-2r} \\ 0_{n-2r\times 2r} & 0_{n-2r\times n-2r} \end{pmatrix}, \quad \text{where } A = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \end{pmatrix}.$$

Proof. Let $f_1 \wedge g_1 + \cdots + f_s \wedge g_s$ be an expression for Ω_b with the fewest number of terms. We mean that there is no expression $\Omega_b = \sum_{i=1}^{t} \varphi_i \wedge \psi_i$ with $t < s$. We note that $\{f_1, g_1, \ldots f_s, g_s\}$ is a linearly independent set in V^*: for any relation of linear dependence between these vectors will yield an expression for Ω_b with $t < s$ terms. Extending $\{f_1, g_1, \ldots f_s, g_s\}$ to a basis $e^1, \ldots, e^n$ of V^*, we see that the matrix of b wrt the dual basis is the canonical form matrix B above. □

If $e'_1, \ldots e'_n$ is another basis of V with the property that the change of basis matrix $P \in GL_n(F)$ is defined by

$$[e_1, \ldots e_n] = [e'_1, \ldots, e'_n]P,$$

then we know that the components $(a_1, \ldots, a_n)$ and $(a'_1, \ldots, a'_n)$ of a vector $v \in V$ wrt these bases are related by $\begin{pmatrix} a'_1 \\ \vdots \\ a'_n \end{pmatrix} = P \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. Similarly, the components $(\alpha_1, \ldots, \alpha_n)$ and $(\alpha'_1, \ldots, \alpha'_n)$ of a vector $f \in V^*$ wrt these bases are related by $\begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} = P^{-\top} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. Similarly, the matrices B and B' of b wrt these bases are related by $B' = QBQ^t$ where $Q = P^{-\top}$. We want to point out that if we expand $\sum B_{ij} e^i \wedge e^j$ using the expressions for $e^j = \sum_i e'^i Q_{ij}$ where $Q = P^{-\top}$ we just obtain $\sum B'_{ij} e^{i'} \wedge e^{j'}$.

1.3.2 Pfaffian

Let $n = 2k$ be an even integer and let $R = \mathbb{Z}[X_{12}, \ldots, X_{n-1,n}]$ be the polynomial ring in $\binom{n}{2}$ variables $\{X_{ij} \colon 1 \le i < j \le n\}$ with integer coefficients. Let X be a generic alternating $n \times n$ matrix, i.e. its $\binom{n}{2}$ entries X_{ij} are indeterminates. Note that $\det(X)$ is a polynomial in the indeterminates X_{ij} with coefficients being ± 1.

Examples: if $n = 2$ then $X = X_{12}J$ where $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $\det(X) = X_{12}^2$.
If $n = 4$ then

$$X = \begin{pmatrix} 0 & X_{12} & X_{13} & X_{14} \\ -X_{12} & 0 & X_{23} & X_{24} \\ -X_{13} & -X_{23} & 0 & X_{34} \\ -X_{14} & -X_{24} & -X_{34} & 0 \end{pmatrix},$$

and it can be checked that

$$\det(X) = (X_{12}X_{34} - X_{13}X_{24} + X_{14}X_{23})^2.$$

Theorem 1.3.3. *Let $n = 2k$ and X be as above. There is a degree k homogeneous polynomial in $Z[X_{12}, \ldots, X_{n-1,n}] = R$ known as the Pfaffian of X and denoted $Pf(X)$ with the property that $det(X) = Pf(X)^2$.*

Let S be any commutative ring, and let A be a $n \times n$ alternating matrix with entries in S, then $det(A)$ is a square in S.

Proof. The second assertion easily follows from the first assertion: Consider the ring homomorphism $f : R \to S$ defined by mapping $f(X_{ij}) = A_{ij}$. Clearly $f(\det(X)) = \det(S)$. Since f is a ring homomorphism and $\det(X) = \mathrm{Pf}(X)^2$, we get $\det(S) = f(\mathrm{Pf}(X))^2$.

We now prove the first assertion. We recall that R is a UFD by Gauss Lemma. Let K be the fraction field of R. We know there is a $P \in GL_n(K)$ such that $PXP^t = \mathrm{diag}(J, \ldots, J)$. Let $\det(P) = f/g$ where $f, g \in R$ are coprime. Since $\det(J) = 1$, We get

$$f^2 \det(X) = g^2 \quad \text{in } R$$

Since f, g are coprime, it follows that g^2 divides $\det(X)$ in R. Therefore $f^2 \cdot (\det(X)/g^2) = 1$. Since the only units in R are ± 1, it follows that $f^2 = 1$ and hence $\det(X) = g^2$ in R. Thus, we have shown that $\det(X)$ is always a square in R. The square root g is the Pfaffian of X. □

1.4 Hermitian and Symmetric Forms

Definition. A Hermitian form satisfies $b(u, v) = b(v, u)^\sigma$, with $\sigma^2 = \mathrm{id}$, $\sigma \neq \mathrm{id}$.

Theorem 3.11. A maximum totally isotropic subspace of a non-degenerate Hermitian form has dimension $\left\lfloor \frac{k}{2} \right\rfloor$.

Theorem 3.12. If b is a non-degenerate Hermitian form, then

$$V_k(F_q) = E_1 \oplus \cdots \oplus E_r \oplus F,$$

where E_i are hyperbolic subspaces and F is either $\{0\}$ or a one-dimensional non-isotropic subspace.

Corollary 3.13. In a suitable basis,

$$b(u, v) = u_1 v_2^\sigma + u_2 v_1^\sigma + \cdots + u_{2r-1} v_{2r}^\sigma + u_{2r} v_{2r-1}^\sigma,$$

with an additional term $u_{2r+1} v_{2r+1}^\sigma$ if k is odd.

Corollary 3.14. All non-degenerate Hermitian forms on $V_k(F_q)$ are equivalent.

Definition. A bilinear form is symmetric if $b(u, v) = b(v, u)$ for all u, v.

Theorem 3.15. If the characteristic of F is 2, any symmetric bilinear form on $V_k(F)$ decomposes as:

$$V_k(F) = E \oplus F,$$

where $b|_E$ is alternating and F is either trivial or a non-isotropic 1-dimensional subspace.

Corollary 3.16. In characteristic 2, a non-degenerate symmetric form b can be written (in a suitable basis) as:

$$b(u, v) = \sum_{i=1}^{r} (u_{2i-1} v_{2i} + u_{2i} v_{2i-1}) + u_{2r+1} v_{2r+1},$$

if $k = 2r + 1$, or without the last term if $k = 2r$.

1.5 Quadratic Forms

Definition 1.5.1. A quadratic form f on $V_k(F)$ is a function $f : V_k(F) \to F$ satisfying:

1. $f(\lambda u) = \lambda^2 f(u)$ for all $\lambda \in F$.
2. The function
$$b(u, v) = f(u + v) - f(u) - f(v)$$
is a bilinear form on $V_k(F)$.

Definition 1.5.2. A quadratic form f is degenerate if there exists a nonzero $u \in V_k(F)$ such that
$$f(u) = 0 \quad \text{and} \quad b(u, v) = 0 \quad \text{for all } v \in V_k(F).$$

Definition 1.5.3. A hyperbolic subspace with respect to a quadratic form is a two-dimensional subspace $\langle u, v\rangle$ such that:
$$f(u) = f(v) = 0 \quad \text{and} \quad b(u, v) \neq 0.$$

Theorem 1.5.4. *If f is a non-degenerate quadratic form on $V_k(F)$, then*
$$V_k(F) = \bigoplus_{i=1}^{r} E_i \oplus X,$$
where X is a non-singular subspace and E_i are hyperbolic subspaces satisfying
$$E_i^{\perp} = \bigoplus_{j \neq i} E_j \oplus X.$$

Isometry with Respect to a Quadratic Form

Let $V_{\mathbb{F}}(f)$ be a vector space over a field $\mathbb{F}$ equipped with a quadratic form f. A **linear map** $\sigma : V_{\mathbb{F}}(f) \to V_{\mathbb{F}}(f)$ is called an **isometry** if:
$$f(\sigma(v)) = f(v) \quad \text{for all } v \in V_{\mathbb{F}}(f).$$

If $b(u, v)$ is the symmetric bilinear form associated with f, then an isometry also satisfies:
$$b(\sigma(u), \sigma(v)) = b(u, v) \quad \text{for all } u, v \in V_{\mathbb{F}}(f).$$

Lemma 3.3.22. For any non-singular vector $v \in V_{\mathbb{F}}$,
$$\sigma_v(w) = w - \frac{b(v, w)}{f(v)} v$$
is an isometry.

Proof. By direct calculation:
$$\begin{aligned} f(\sigma_v(w)) &= f\left(w - \frac{b(v, w)}{f(v)} v\right) \\ &= f(w) + \left(\frac{b(v, w)^2}{f(v)^2}\right) f(v) - \left(\frac{b(v, w)}{f(v)}\right)^2 f(v) \\ &= f(w). \end{aligned}$$

Lemma 3.3.23. For any two singular linearly independent vectors u and v, there is an isometry α such that $\alpha(u) = v$.

Proof. If $b(u,v) \neq 0$, then $u+v$ is non-singular. Let

$$w = u + \frac{f(u+v)}{b(u,v)}v.$$

Then the composition $\alpha = \sigma_w\sigma_v\sigma_u$ is the required isometry such that $\alpha(u) = v$.

Lemma 3.3.24. For any isometry α and vector v, we have:

$$\sigma_{\alpha(v)} = \alpha\sigma_v\alpha^{-1}.$$

Proof. Since $f(\alpha(v)) = f(v)$, it follows that:

$$b(u,v) = b(\alpha(u),\alpha(v)) \quad \text{for all } u,v \in V_{\mathbb{F}}.$$

Then,

$$\alpha\left(v - \frac{b(v,w)}{f(v)}v\right) = \alpha(v) - \frac{b(\alpha(v),\alpha(w))}{f(\alpha(v))}\alpha(v) = \sigma_{\alpha(v)}(\alpha(w)).$$

Theorem 3.25. A maximum totally singular subspace U has dimension $\frac{k-\dim X}{2}$, where X is a maximal non-singular subspace.

Chapter 2

The Basic Linear Group

Topics Covered

We have started reading a new book and postponed Chapter 4 of Simion Ball [**Ball**]. The new book is:

> American Mathematical Society, Graduate Studies in Mathematics, Volume 39: *Classical Groups and Geometric Algebra* by Larry C. Grove [**Grove**].

We have covered Chapter 1, which discusses the basic linear groups. This book assumes basic knowledge of group theory, linear algebra, and some familiarity with finite fields.

basic setting

Let V be an n-dimensional vector space over a field F. (Observe that we have not made any assumptions about the type of field.)

The general linear group, denoted $GL(V)$, consists of all invertible linear transformations on V:

$$GL(V) = \{A \in \mathrm{Mat}(n, F) \mid \det(A) \neq 0\}.$$

The determinant map is defined as:

$$\det : GL(V) \to F^*,$$

where $F^* = F \setminus \{0\}$.

Observe that the determinant map is a homomorphism, and its kernel is given by:

$$\ker(\det) = \{A \in GL(V) \mid \det(A) = 1\} = SL(V).$$

This is called the *special linear group*.

A hyperplane in V is a subspace of dimension $n - 1$ (i.e., of codimension 1). A transvection $\tau \in GL(V)$ is a linear transformation such that there exists a hyperplane $W \subset V$ satisfying the following properties: $\tau|_W = \mathrm{Id}|_W$, meaning τ acts as the identity on W. And For all $v \in V$, the difference $\tau v - v$ belongs to W.

Then subspace W is called the fixed hyperplane of τ.

A good example of a transvection is a shear transformation. The edge along which it shears is the hyperplane on which the transformation acts as the identity.

2.1 Projective Spaces And Hyperplanes

2.1.1 Centers of $GL(n, F)$ and $SL(n, V)$

The center of $GL_n(F)$ consists of those $A \in GL_n(F)$ which commute with all $B \in GL_n(F)$. Taking $B = I + E_{\mu\nu}$ for some $\mu \neq \nu$, and considering the ij-th entry of $AB = BA$, we get

$$A_{ij} + A_{i\mu}\delta_{j\nu} = A_{ij} + A_{\nu j}\delta_{i\mu}$$

Taking $j = \nu$ and $i \neq \mu$, we get $A_{i\mu} = 0$, which shows that A is a diagonal matrix $\mathrm{diag}(a_1, \ldots, a_n)$. Next, taking $i = \mu$ and $j = \nu$, we get $a_i = a_j$. Thus, A is a scalar matrix. This completes the proof that

$$Z(GL_n(F)) = \{aI_n \colon a \in F^\times\}.$$

Now, let $A \in Z(SL_n(F))$. Since $B = I + E_{\mu\nu} \in SL_n(F)$, the above argument shows that $A = aI_n$ again. For aI_n to be in $SL_n(F)$, we must have a to be an n-th root of unity in F. Thus

$$Z(SL_n(F)) = \{aI_n \colon a^n = 1\}.$$

2.2 projective space

If $0 \neq v \in V$ write $[v]$ for the line $Fv = \langle v \rangle$ through the origin spanned by v, and call it a *projective point*. The set of all distinct projective points $[v]$ is called the *projective space* of dimension $n-1$ based on V, and is denoted by $\mathbb{P}_{n-1}(V)$, or simply by $\mathbb{P}(V)$. There is a natural permutation action of $\mathrm{GL}(V)$ on $\mathbb{P}(V)$, given by $\tau[v] = [\tau v]$ for all $\tau \in \mathrm{GL}(V)$, $[v] \in \mathbb{P}(V)$. the kernel of the action is $Z(\mathrm{GL}(V))$, and likewise that the kernel of the action of $\mathrm{SL}(V)$ on $\mathbb{P}(V)$ is $Z(\mathrm{SL}(V))$.

We also observe that:

- Lines passing through the origin correspond to points in the projective space.
- If V is two-dimensional, then the projective space $\mathbb{P}(V)$ can be thought of as a line with an additional point at infinity, associated with its slope.

Exercise

If $\dim V = n$ and $|F| = q$, finite, show that

$$|\mathbb{P}(V)| = \frac{q^n - 1}{q - 1}.$$

There are isomorphic copies based on the corresponding matrix groups, with obvious corresponding notation.

Proof. The projective space $\mathbb{P}(V)$ consists of 1-dimensional subspaces (lines through the origin) of the n-dimensional vector space V over the finite field F with q elements.

Every nonzero vector $v \in V$ lies on a unique line Fv. Two vectors v and w define the same projective point if and only if $v = \lambda w$ for some nonzero scalar $\lambda \in F^\times$. So, each projective point corresponds to an equivalence class of vectors under scalar multiplication.

There are $q^n - 1$ nonzero vectors in V, and each line contains exactly $q - 1$ of them (one for each nonzero scalar multiple). Thus, the number of 1-dimensional subspaces is

$$|\mathbb{P}(V)| = \frac{q^n - 1}{q - 1}.$$

□

Define the *projective general linear group* of V to be

$$\mathrm{PGL}(V) = \mathrm{GL}(V)/Z(\mathrm{GL}(V))$$

and the *projective special linear group* to be

$$\mathrm{PSL}(V) = \mathrm{SL}(V)/Z(\mathrm{SL}(V));$$

each of them acts faithfully on $\mathbb{P}(V)$.

2.2.1 Action of $GL(V)$ on Projective Space and Möbius Transformations

Understanding the action of $GL(V)$ on projective space leads to a natural connection with Möbius transformations and complex analysis:

- The complex projective line $\mathbb{P}^1(\mathbb{C})$ can be identified with $\mathbb{C} \cup \{\infty\}$.
- This space is the simplest setting where we can perform calculus after $\mathbb{C}^2$ itself.
- Topologically, $\mathbb{C} \cup \{\infty\}$ is homeomorphic to the Riemann sphere S^2.

2.2.2 Visualization of Projective Space in $\mathbb{R}^3$

One way to visualize projective space in $\mathbb{R}^3$ is by considering planes:

- The projective space of a three-dimensional vector space can be described using coordinate charts defined by the planes $X = 1$, $Y = 1$, and $Z = 1$.
- Transition maps between these charts are polynomial functions.
- In the case of $\mathbb{R}^2$, the projective space can be interpreted as a one-point compactification, which has an induced topology.
- This space is topologically homeomorphic to S^2.

2.3 Transvections

$\tau \in GL(V)$ is called a transvection if i) $\tau \neq I_V$, ii) there is a hyperplane $W \subset V$, such that $\tau_{|W} = I_W$ is the identity transformation of W, and iii) the quotient map $\bar{\tau} : V/W \to V/W$ is also the identity transformation of the one-dimensional space V/W.

Exercise 1 Show that the inverse of a transvection is a transvection.
Ans: Clearly, $\tau^{-1}_{|W} = I_W$ and the induced map $\overline{\tau^{-1}} : V/W \to V/W$ is also $I_{V/W}$. Therefore,

τ^{-1} is also a transvection.

Alternative Ans: If τ is a transvection then $\tau w = w$ for all $w \in W$. Multiplying both sides of this equality by $\tau^{-1} \neq 1$ we obtain $\tau^{-1}w = w$ for all $w \in W$. Also, we have $\tau v - v = w \in W$, hence

$$v - \tau^{-1}v = w, \quad \text{so} \quad \tau^{-1}v - v = -w \in W.$$

Thus τ^{-1} is a transvection.

Exercise 2 Suppose that V is a subspace of a space V_1, and $v \in V_1 \setminus V$, and τ is a transvection on V with fixed hyperplane W. Show that τ can be extended to a transvection τ_1 on V whose fixed hyperplane W_1 contains v.
Ans: Let U be a complement of V in V_1, i.e. $V_1 = V \oplus U$. Take $W_1 = W \oplus U$. Let $\tau_1 = \tau \oplus I_U$. (i) Since $\tau \neq I_V$ we get $\tau_1 \neq I_{V_1}$. (ii) Clearly $(\tau_1)_{|W_1} = I_{W_1}$. So τ_1 fixes the hyperplane W_1 of V_1. (iii) Since V_1/W_1 is isomorphic to V/W and the induced map $\overline{\tau_1} : V_1/W_1 \to V_1/W_1$ is isomorphic to the map $\bar{\tau} : V/W \to V/W$ which we know is the identity map. Thus τ_1 is the desired transvection of V_1 whose fixed hyperplane contains v.

Alternative Solution: Let $\{v_1, v_2, \ldots, v_k\}$ be a basis for V such that $\{v_2, \ldots, v_k\}$ is a basis for W. We can choose a basis for V_1 consisting of the following vectors:

$$\{v_1, v_2, \ldots, v_k, v_{k+1} = v, \ldots, v_n\}.$$

Consider a hyperplane W_1 spanned by $\{v_2, \ldots, v_n\}$ and extend τ on V_1 by setting $\tau_1|_V = \tau|_V$, and $\tau_1 v_i = v_i$ for all $i > k$. Then $\tau_1|_{W_1} = 1_{W_1}$ and

$$\tau_1 v_1 - v_1 = \tau v_1 - v_1 \in W \subseteq W_1.$$

So τ_1 is a transvection with fixed hyperplane containing $v_{k+1} = v$.

Proposition 1.2: If u and v are linearly independent in V, then there is a transvection τ with $\tau u = v$.

Proof. If τ is such a transvection, and W is its fixed hyperplane then we know that $\tau(u) = v \neq u$ implies that $u \notin W$ and hence $v + W = \bar{\tau}(u + W) = u + W$. Let $v_1, \ldots, v_n$ be a basis of V such that $v_1 = u$ and $v_2 = v - u$. Let W be the hyperplane spanned by $v_2, \ldots, v_n$ and define τ by $\tau(v_i) = v_i$ for $i > 1$ and $\tau(v_1) = v_1 + v_2$ (so that $\tau(u) = v$). Clearly (i) $\tau \neq I_V$, (ii) τ fixes the hyperplane W, iii) the induced map $\bar{\tau} : V/W \to V/W$ is $I_{V/W}$. Thus τ is the desired transvection. □

Alternative Proof

Proof. Choose a hyperplane W in V with $u - v \in W$ but $u \notin W$, and define τ by

$$\tau|_W = 1_W, \quad \tau u = v.$$

If $x \in V$, write $x = au + w$, where $a \in \mathbb{F}$ and $w \in W$. Then

$$\tau x - x = av + w - au - w = a(v - u) \in W,$$

so τ is a transvection. □

Proposition 1.3: Suppose that W_1 and W_2 are two distinct hyperplanes in V and that $v \in V \setminus (W_1 \cup W_2)$. Then there is a transvection τ with $\tau W_1 = W_2$ and $\tau(v) = v$.

Proof. Let $e_1, \ldots, e_n$ be a basis of V, such that W_1 is the span of $e_1, e_3, \ldots, e_n$ and W_2 is the span of $e_2, \ldots, e_n$. This is possible because $W_1 \cap W_2$ is $n-2$ dimensional. The given vector $v = (a_1, \ldots, a_n)$ with $a_1 a_2 \neq 0$. Rescaling e_1, e_2, we may assume $a_1 = a_2 = 1$. We can write $v = e_1 + e_2 + v_0$ with $v_0 \in W_1 \cap W_2$. Let W be hyperplane which is the span of $e_1 + e_2, e_3, \ldots, e_n$. Define τ by $\tau(e_i) = e_i$ for $i \geq 3$, and $\tau(e_1) = 2e_1 + e_2$, $\tau(e_2) = -e_1$. Then τ fixes $(e_1 + e_2)$ as well as $e_2, \ldots, e_n$, and hence (i) τ fixes the hyperplane W and $v \in W$ as desired, (ii) $\tau \neq I_V$ and $\tau(e_1 + W) = e_2 + W = 2e_1 + e_2 + W = e_1 + W$. The matrix of τ is $\begin{pmatrix} 2 & -1 & \\ 1 & 0 & \\ & & I_{n-2} \end{pmatrix}$ whose determinant is 1 and hence $\tau \in GL(V)$. □

Theorem 1.4: The set of transvections generate $SL(V)$.

Proof. Let $e_1, \ldots, e_n$ be a basis of V. Let $\mathcal{E}$ denote the set of elementary matrix of the first kind, namely atrices of the form $E = I + \lambda E_{ij}$ where $i \neq j$ and $\lambda \in F$, as above. We note the following properties of $\mathcal{E} = I + \lambda E_{ij}$ is the span of $\{e_1, \ldots, e_n\} \setminus e_j$.

1. Each $E \neq I_n \in \mathcal{E}$ is a transvection. The fixed hyperplane of $E = I + \lambda E_{ij}$ is the span of $\{e_1, \ldots, e_n\} \setminus e_j$.

2. For fixed i, j the map $\lambda \mapsto (I + \lambda E_{ij})$ is isomorphism of the additive abelian group $(F, +)$ and the multiplicative abelian $\{I + \lambda E_{ij} \colon \lambda \in F\}$. In particular, the inverse of E equals $I - \lambda E_{ij}$ is in $\mathcal{E}$

3. For $E = I + \lambda E_{ij}$ and a $n \times n$ matrix A, we note that $A \mapsto EA$ changes the i-th row $R_i(A)$ of A to $R_i(A) + \lambda R_j(A)$ while keeping the other rows unchanged. Similarly, $A \mapsto AE$ has the effect $C_j(A) \mapsto C_j(A) + \lambda C_i(A)$.

We will show that for any $A \in SL_n(F)$ there exist matrices P, Q which are products of matrices in $\mathcal{E}$, and hence A is a product of (inverses of) matrices in $\mathcal{E}$. Since the first column of A is nonzero, we can easily find a matrix $E \in \mathcal{E}$ so that $A' = EA$ has the property that $A_{n1} \neq 0$. Let $E' = I + \lambda E_{1n}$ where $\lambda = (1 - A_{11})/A_{n1}$. We have $B = E'A'$ has the property that $B_{11} = 1$. Let $B' = E_2 \ldots E_n B$ where $E_i = I - A_{i1} E_{i1}$. Note that the first column of $B' = (1, 0, \ldots, 0)^\top$. Similarly, $B'' = B' E_2' E_3' \ldots E_n'$ for suitable $E_j' \in \mathcal{E}$ has the property that $B'' = \left(\begin{smallmatrix} 1 & 0 \\ 0 & C \end{smallmatrix}\right)$ for $C \in SL_{n-1}(F)$, Inductively we can write C as a product of $n-1 \times n-1$ elementary matrices of first kind (which can be embedded in $\mathcal{E}$ as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & E' \end{smallmatrix}\right)$). This completes the proof that $\mathcal{E}$ generates $SL_n(F)$. □

Proposition 1.5 and 1.6: Any transvection of V is conjugate in $SL(V)$ to $E_\lambda = I + \lambda E_{21}$. If $n > 2$ we can take $\lambda = 1$, and hence all transvections are conjugate in $SL(V)$

Proof. If τ is a transvection with fixed hyperplane W, then writing $V = U \oplus W$ for some one-dimensional complement of W, and taking $e_1, \ldots, e_n$ to be a basis of V adapted to the decomposition $V = U \oplus W$ we see that the matrix of τ wrt this basis is $A = \left(\begin{smallmatrix} 1 & 0 \\ w & I_{n-1} \end{smallmatrix}\right)$ for some nonzero $w \in W$. Let $f_1 = e_1$, and let $f_2, \ldots, f_n$ be a basis of W with $f_2 = w$. Let $P \in GL_n(F)$ denote the change of basis matrix from $e_1, \ldots, e_n$ to $f_1, \ldots, f_n$. The matrix of τ wrt the new basis $f_1, \ldots, f_n$ is

$$PAP^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & I_{n-1} \end{smallmatrix}\right) = I + E_{21}.$$

This shows that any two transvections are conjugate in $GL(V)$. However if we assume $n > 2$, then we may simply rescale f_n so that P has determinant one, to conclude that any two transvections are conjugate in $SL(V)$.

Note: Proposition 1.6 is already covered in the form $A = \left(\begin{smallmatrix} 1 & 0 \\ w & I_{n-1} \end{smallmatrix}\right)$ for some nonzero $w \in W$. □

Theorem 1.7. If $n \geq 3$ then $SL(V)$ equals its commutator subgroup.

Proof. Similar to the proof in the book, we take $\tau_1 = I + E_{21}$ and $\tau_2 = I + E_{32}$. Since $E_{21}E_{32} = 0$ and $\tau_1^{-1} = I - E_{21}, \tau_2^{-1} = I - E_{32}$, we see that

$$\tau_1\tau_2 = I + E_{21} + E_{32}, \quad \tau_1^{-1}\tau_2^{-1} = I - E_{21} - E_{32}.$$

Using the fact that $E_{ij}E_{k\ell}$is the zero matrix unless $k = j$ in which case it is $E_{i\ell}$, we conclude that

$$\tau_1\tau_2\tau_1^{-1}\tau_2^{-1} = I + E_{21} + E_{32} - E_{21} - E_{31} - E_{32} = I - E_{31},$$

which is a transvection. Since all transvections are conjugate in $SL(V)$ for $n \geq 3$, and the commutator subgroup G' is a normal subgroup, we see that G' contains all transvections, and hence all of $SL(V)$. □

Theorem 1.9. If $G = SL_2(F)$ and $|F| \neq \{2, 3\}$ then $G' = G$.
If $F = F_q$ with $q = 2$ then $G = SL_2(2) \simeq S_3$ and $G' = A_3$.

Proof. Following the proof in the book, if $|F| \neq \{2, 3\} > 2$ it is possible to pick $a \in F^\times$ such that $a^2 \neq 1$. Then

$$\left(\begin{smallmatrix} a^{-1} & \\ & a \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & \\ & a^{-1} \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ -\lambda & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ \lambda(a^2-1) & 1 \end{smallmatrix}\right).$$

Since λ was arbitrary, we see that G' contains $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ for all b, and we have shown previously that any transvection is conjugate in $SL_2(F)$ to $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ for all b for some $b \in F^\times$. Using the normality of G', we conclude G' contains all transvections and hence all of $SL_2(F)$.

If $F = F_q$ with $q = 2$, then the size of $SL_2(2)$ is 6 and it is non-abelian. Therefore it must be isomorphisc to S_3, and its commutator group is isomorphic to A_3

□

Some Results

1. If τ_1 and τ_2 are transvections on V, then they are conjugate in $\mathrm{GL}(V)$. If $\dim V > 2$, then they are conjugate in $\mathrm{SL}(V)$.

2. Suppose that $\dim V = 2$, and let $\{v_1, v_2\}$ be any basis for V. Then every transvection is conjugate in $\mathrm{SL}(V)$ to one whose matrix relative to the basis $\{v_1, v_2\}$ is of the form
$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \quad \text{for some } a \in \mathbb{F}.$$

3. except for PSL(2, 2) and PSL(2, 3) every PSL(V) is a simple group.

Chapter 3

Bilinear Forms

3.1 Notation

Let V be a vector space over a field F. The dual space of V, denoted V^*, is defined as $V^* = \mathrm{Hom}_F(V, F)$, which is the set of all linear functionals from V to F. If $\{v_1, v_2, \ldots, v_n\}$ is a basis for V, then the dual basis $\{v_1^*, v_2^*, \ldots, v_n^*\}$ for V^* is defined by:

$$v_i^*(v_j) = \delta_{i,j} \quad \text{for all } i, j \in \{1, 2, \ldots, n\},$$

where $\delta_{i,j}$ is the Kronecker delta. When V is finite-dimensional, $\dim_F(V^*) = \dim_F(V)$.

3.2 Bilinear Forms

A bilinear form on V is a function $B : V \times V \to F$ that is linear in both variables. That is, for all $v, w, u \in V$ and $\alpha \in F$, the following hold:

$$B(v + w, u) = B(v, u) + B(w, u), \quad B(\alpha v, w) = \alpha B(v, w),$$

$$B(v, w + u) = B(v, w) + B(v, u), \quad B(v, \alpha w) = \alpha B(v, w).$$

If B is a bilinear form and $\{v_1, v_2, \ldots, v_n\}$ is a basis for V, then the matrix associated with B is $\hat{B} = [b_{ij}]$, where:

$$b_{ij} = B(v_i, v_j) \quad \text{for all } i, j.$$

If $\{w_1, w_2, \ldots, w_n\}$ is another basis for V, then:

$$B(w_i, w_j) = \sum_{k,l} d_{ki} B(v_k, v_l) d_{lj} = \sum_{k,l} d_{ki} b_{kl} d_{lj},$$

where $D = [d_{ij}]$ is the change of basis matrix. The ij-th entry of the matrix representation of B with respect to the new basis is given by $(D^T \hat{B} D)_{ij}$. Note that D is invertible. Two matrices M and N are called *congruent* if there exists an invertible matrix D such that $M = D^T N D$.

Linear Maps Associated with Bilinear Forms

If B is a bilinear form on V, we can define two linear maps $L : V \to V^*$ and $R : V \to V^*$ as follows:

$$L(v) = L_v \quad \text{and} \quad R(v) = R_v,$$

where L_v and R_v are defined by fixing the vector in the bilinear form:

$$L_v(w) = B(v, w) \quad \text{and} \quad R_v(w) = B(w, v) \quad \text{for all } w \in V.$$

Since B is bilinear and linear in both variables, it is straightforward to verify that L and R are linear transformations.

We say that a bilinear form is *degenerate* if the determinant of the matrix associated with the bilinear form is zero and *non-degenerate* if it is non-zero.

Tensor Product Construction

The tensor product construction turns bilinear maps into linear maps. If we have a bilinear form

$$B : V \times V \to \mathbb{F},$$

we obtain a linear map

$$T_B : V \otimes_{\mathbb{F}} V \to \mathbb{F}$$

characterized by its values on simple tensors:

$$T_B(v \otimes w) = B(v, w).$$

While L and R both map V to V^*, the map T_B maps $V \otimes_{\mathbb{F}} V$ to $\mathbb{F}$. Conversely, from any linear map

$$T : V \otimes_{\mathbb{F}} V \to \mathbb{F}$$

we get a bilinear form

$$B_T : V \times V \to \mathbb{F} \quad \text{by} \quad B_T(v, w) = T(v \otimes w).$$

The correspondences $B \mapsto T_B$ and $T \mapsto B_T$ are bijections between the bilinear forms on V and the linear maps $V \otimes_{\mathbb{F}} V \to \mathbb{F}$. Since linear maps to $\mathbb{F}$ correspond to elements of the dual space, the space $\mathrm{Bil}(V)$ of all bilinear forms on V is naturally identifiable with

$$(V \otimes_{\mathbb{F}} V)^*,$$

which is naturally isomorphic to

$$V^* \otimes_{\mathbb{F}} V^* = (V^*)^{\otimes 2}$$

via the identification

$$(\varphi \otimes \psi)(v \otimes w) = \varphi(v)\psi(w).$$

Thus, the bilinear forms on V are the elements of $(V^*)^{\otimes 2}$.

Natural Isomorphisms

Returning to L_v and R_v, consider the choice between them by thinking about a general bilinear map $V \times V \to V$, where V is an F-vector space. Such a bilinear map corresponds to a linear map $V \otimes_F V \to V$, and there are natural isomorphisms:

$$\mathrm{Hom}_F(V \otimes_F V, V) \cong \mathrm{Hom}_F(V, \mathrm{Hom}_F(V, V)).$$

The first isomorphism turns $f \in \mathrm{Hom}_F(V \otimes_F V, V)$ into $v \mapsto [w \mapsto f(v \otimes w)]$, and the second isomorphism turns f into $w \mapsto [v \mapsto f(v \otimes w)]$. When $U = F$, these are the two different isomorphisms $(V \otimes_F V)^* \to \mathrm{Hom}_F(V, V^*)$ by $B \mapsto L_v$ and $B \mapsto R_v$. In the most general setting, though, L_v and R_v are analogues of linear maps between different spaces.
Given a bilinear form B on V and subsets $S, T \subseteq V$, we define:

$$\perp_L (S) = \{v \in V : B(v, w) = 0, \text{ all } w \in S\},$$

$$\perp_R (S) = \{v \in V : B(w, v) = 0, \text{ all } w \in S\}.$$

Theorem. *Show That $\perp_L (S)$ and $\perp_R (S)$ are subspaces of V*

Proof. For $\perp_L (S)$:
Zero vector: $0 \in \perp_L (S)$ since $B(0, w) = 0$ for all $w \in S$.
Closed under addition: If $v_1, v_2 \in \perp_L (S)$, then for any $w \in S$,

$$B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w) = 0 + 0 = 0,$$

so $v_1 + v_2 \in \perp_L (S)$.
Closed under scalar multiplication: If $v \in \perp_L (S)$ and $\lambda \in \mathbb{F}$, then for any $w \in S$,

$$B(\lambda v, w) = \lambda B(v, w) = \lambda \cdot 0 = 0,$$

so $\lambda v \in \perp_L (S)$.
For $\perp_R (S)$: The proof is identical, replacing $B(v, w)$ with $B(w, v)$. □

Theorem. *Show that $\perp_L (\perp_R (S)) \supseteq S$ and $\perp_R (\perp_L (S)) \supseteq S$*

Proof. Let $s \in S$.
For all $v \in \perp_R (S)$, by definition $B(v, s) = 0$. Hence, $s \in \perp_L (\perp_R (S))$.
For all $v \in \perp_L (S)$, by definition $B(s, v) = 0$. Hence, $s \in \perp_R (\perp_L (S))$.
Therefore, $S \subseteq \perp_L (\perp_R (S))$ and $S \subseteq \perp_R (\perp_L (S))$. □

Theorem. *Show that if $S \subseteq T$, then $\perp_L (T) \subseteq \perp_L (S)$ and $\perp_R (T) \subseteq \perp_R (S)$*

Proof. For $\perp_L$: If $v \in \perp_L (T)$, then $B(v, w) = 0$ for all $w \in T$. Since $S \subseteq T$, this implies $B(v, w) = 0$ for all $w \in S$. Thus, $v \in \perp_L (S)$.
For $\perp_R$: If $v \in \perp_R (T)$, then $B(w, v) = 0$ for all $w \in T$. Since $S \subseteq T$, this implies $B(w, v) = 0$ for all $w \in S$. Thus, $v \in \perp_R (S)$. □

Proposition 2.6. *Suppose that B is a bilinear form on V satisfying*

$$B(u,v)B(w,u) = B(v,u)B(u,w) \quad (*)$$

for all $u, v, w \in V$. Then B is symmetric or alternating.

Proof. Take $u = v$ in $(*)$ and conclude that

$$B(v,v)[B(w,v) - B(v,w)] = 0 \quad (**)$$

for all $v, w \in V$. We wish to show that either $B(v,v) = 0$ for all $v \in V$, or $B(u,v) = B(v,u)$ for all $u, v \in V$. Suppose, for contradiction, that there exist $x, y, z \in V$ with $B(y,y) \neq 0$ and $B(x,z) \neq B(z,x)$. Applying $(**)$, we obtain:

(i) $B(x,x) = B(z,z) = 0$.

Proof: Since $B(x,z) - B(z,x) \neq 0$, applying $(**)$ with $v = x$ and $w = z$ gives

$$B(x,x)[B(x,z) - B(z,x)] = 0.$$

Since the second term is nonzero and we are in a field (which is an integral domain), it follows that $B(x,x) = 0$. Similarly, applying $(**)$ with $v = z$ and $w = x$, we get $B(z,z) = 0$.

(ii) $B(x,y) = B(y,x)$.

Proof: Setting $v = y$ and $w = x$ in $(**)$ gives

$$B(y,y)[B(x,y) - B(y,x)] = 0.$$

Since $B(y,y) \neq 0$, we conclude that $B(x,y) = B(y,x)$.

(iii) $B(y,z) = B(z,y)$.

Proof: This follows similarly to (ii) by taking $v = y$ and $w = z$ in $(**)$.

Using $(*)$ with $u = x$, $v = y$, and $w = z$, and applying (ii), we get

$$B(x,y)B(z,x) = B(y,x)B(x,z).$$

Since $B(y,x) = B(x,y)$, this simplifies to

$$B(x,y)[B(x,z) - B(z,x)] = 0.$$

Since the second term is nonzero, it follows that $B(x,y) = 0 = B(y,x)$. A similar argument shows that $B(y,z) = 0 = B(z,y)$.

Now, interchange u and w in $(*)$ and use $u = x$, $v = y$, and $w = z$ again. From (iii), we get $B(z,y) = B(y,z) = 0$, so that

$$B(x,y+z) = B(x,z) \neq B(z,x) = B(y+z,x).$$

By $(**)$,

$$B(y+z,y+z)[B(x,y+z) - B(y+z,x)] = 0.$$

Since the second term is nonzero, we obtain $B(y+z,y+z) = 0$, leading to

$$B(y+z,y+z) = B(y,y) + B(y,z) + B(z,y) + B(z,z).$$

Since $B(y,z) = B(z,y) = 0$ and $B(z,z) = 0$, we get

$$B(y+z,y+z) = B(y,y) \neq 0,$$

which is a contradiction. This completes the proof. $\square$

Some Results:

- **Proposition 2.7.** A bilinear form B on V is reflexive if and only if it is either symmetric or alternate.
- **Proposition 2.8.** Bilinear forms B_1, B_2 on spaces V_1, V_2 are equivalent if and only if there are bases for V_1, V_2 relative to which $\widehat{B_1} = \widehat{B_2}$.
- **Proposition 2.9.** Suppose that B is a reflexive bilinear form on V, and that W is a nondegenerate subspace of V. Then $V = W \oplus W^{\perp}$.
- **Theorem 2.10.** If B is an alternating form on V, then

  $$V = W_1 \oplus W_2 \oplus \cdots \oplus W_r \oplus \operatorname{rad} V,$$

  a direct sum of mutually orthogonal subspaces, with each W_i a hyperbolic plane.
- **Corollary 2.11.** B has even rank; if B is nondegenerate then $\dim V$ is even.
- **Corollary 2.12.** Alternate bilinear forms B_1 and B_2 on spaces V_1 and V_2 are equivalent if and only if $\dim V_1 = \dim V_2$ and $\operatorname{rank} B_1 = \operatorname{rank} B_2$.
- **Corollary 2.13.** The determinant of any representing matrix for an alternating form is a square in F.

Chapter 4

Symplectic groups

The general setting is

(1)(a) $V = 2n$-dimensional vector space over a field F ,

(1)(b) $B =$ non-degenerate symplectic form on V .

(1)(c) $Sp(V) = \{g \in GL(V) \mid B(gv, gw) = B(v, w)(v, w \in V)\}$.

This is the symplectic group of the form B. The goal is to work out the structure of certain subgroups of $Sp(V)$, and to use that structure to calculate the orders of symplectic groups over finite fields. Recall first of all the projective space
(2) $P(V) =$ set of lines in V .
If u is a non-zero vector in V, we write $[u] = \{au \mid a \in F\}$ for the line through u. The group $Sp(V)$ (like any subgroup of $GL(V)$) acts on $P(V)$.
Lemma 3 (text, Proposition 3.2). The action of $Sp(V)$ on $V - \{0\}$ is transitive; consequently the action on $P(V)$ is transitive as well.
From now on we fix a non-zero vector $u \in V$. (Such a vector exists if $n \geq 1$.) The goal is to understand the group

$$\begin{aligned} StabSp(V)([u]) &= \{g \in Sp(V) \mid g[u] = [u]\}(4) \\ &= \{g \in Sp(V) \mid gu = ku, \text{ some } k \in F^\times\}. \end{aligned}$$

There at least three reasons to understand this group. First, when F is a finite field we can use the formula

$$|Sp(V)| = |P(V)| \cdot |StabSp(V)([u])|$$

to compute the order of the symplectic group.
In a symplectic space (V, B) over F, recall that a transvection $\tau \in \mathrm{Sp}(V)$ with fixed hyperplane W has $W^\perp = \langle u \rangle$, $\dim W^\perp = 1$, $u^\perp = W$, $u \in W$. Decompose $V = \langle x \rangle \oplus W$, $x \notin W$, so $\tau x - x = z \in W$. For $v = bx + w$, $b \in F$, $w \in W$, define $f(v) = b$, $\ker f = W$. There exists $y \in V$ such that $f(v) = B(v, y)$:

$$\tau v = v + B(v, y)z.$$

Since $B(w, y) = 0$ for $w \in W$, $y = cu \in W^\perp$, $c \in F^*$. Also, $B(w, z) = 0$, so $z = du$, $d \in F^*$. Thus:

$$\tau v = v + cdB(v, u)u = \tau_{u,a}(v), \quad a = cd.$$

Conversely, $\tau_{u,a}(v) = v + aB(v,u)u$ for $u \neq 0$, $a \in F$, is a transvection in $\mathrm{Sp}(V)$ with fixed hyperplane $u^\perp$.

We first verify that these maps satisfy the following properties:

$$\tau_{u,a}\tau_{u,b} = \tau_{u,a+b}, \quad \tau_{bu,a} = \tau_{u,ab^2}, \quad \tau_{u,a}^{-1} = \tau_{u,-a}.$$

To see the first identity, compute:

$$\tau_{u,b}(v) = v + bB(v,u)u,$$

$$\tau_{u,a}(\tau_{u,b}(v)) = \tau_{u,a}(v + bB(v,u)u) = v + bB(v,u)u + aB(v + bB(v,u)u, u)u.$$

Using bilinearity and the alternating property $B(u,u) = 0$, we obtain:

$$B(v + bB(v,u)u, u) = B(v,u) + bB(v,u)B(u,u) = B(v,u),$$

hence

$$\tau_{u,a}(\tau_{u,b}(v)) = v + (a+b)B(v,u)u = \tau_{u,a+b}(v),$$

so that $\tau_{u,a}\tau_{u,b} = \tau_{u,a+b}$.

Next, we consider the identity $\tau_{bu,a} = \tau_{u,ab^2}$. We compute:

$$\tau_{bu,a}(v) = v + aB(v,bu)bu = v + abB(v,u) \cdot bu = v + ab^2B(v,u)u = \tau_{u,ab^2}(v).$$

For the inverse, since $\tau_{u,a}\tau_{u,b} = \tau_{u,a+b}$, the inverse of $\tau_{u,a}$ must be $\tau_{u,-a}$ because

$$\tau_{u,a}\tau_{u,-a} = \tau_{u,0},$$

which is the identity map on V. Thus, $\tau_{u,a}^{-1} = \tau_{u,-a}$.

We now observe that the set $\{\tau_{u,a} : a \in F\}$ forms a group under composition. Indeed, it is closed under composition, the identity is $\tau_{u,0}$, every element has an inverse, and composition is associative. Define a map $\phi : F \to \{\tau_{u,a}\}$ by $\phi(a) = \tau_{u,a}$. Then

$$\phi(a+b) = \tau_{u,a+b} = \tau_{u,a}\tau_{u,b} = \phi(a)\phi(b),$$

so ϕ is a homomorphism. If $\phi(a) = \phi(b)$, then $\tau_{u,a} = \tau_{u,b}$, and for all $v \in V$,

$$(a-b)B(v,u)u = 0.$$

Since $u \neq 0$ and B is nondegenerate, there exists v with $B(v,u) \neq 0$, implying $a = b$. Thus, ϕ is injective. Surjectivity is immediate from the definition. Therefore, $\{\tau_{u,a}\} \cong (F,+)$.

Finally, if $\sigma \in \mathrm{Sp}(V)$, the symplectic group preserving B, then

$$\sigma\tau_{u,a}\sigma^{-1}(v) = \sigma\left(\tau_{u,a}(\sigma^{-1}v)\right) = \sigma\left(\sigma^{-1}v + aB(\sigma^{-1}v,u)u\right) = v + aB(\sigma^{-1}v,u)\sigma u.$$

Since σ preserves B, we have

$$B(\sigma^{-1}v,u) = B(v,\sigma u),$$

and so

$$\sigma\tau_{u,a}\sigma^{-1}(v) = v + aB(v,\sigma u)\sigma u = \tau_{\sigma u,a}(v).$$

Thus, $\sigma\tau_{u,a}\sigma^{-1} = \tau_{\sigma u,a}$.

some other thoerems we covered.

Theorem 4.0.1 (Proposition 3.3)**.** *If V is a symplectic space, then the group $\mathcal{T} \leq \mathrm{Sp}(V)$, generated by symplectic transvections, is transitive on the set $\mathcal{S}$ of all hyperbolic pairs in V.*

Theorem 4.0.2 (Theorem 3.4)**.** *The symplectic group $\mathrm{Sp}(V)$ is generated by transvections.*

Theorem 4.0.3 (Proposition 3.6)**.** *The center of $\mathrm{Sp}(V)$ is ± 1.*

Chapter 5

Symmetric Forms and Quadratic Forms

Assume for this chapter that F is a field with char $F \neq 2$. Recall from Chapter 2 that a bilinear form B on a vector space V over F is symmetric if $B(u,v) = B(v,u)$ for all $u, v \in V$. Thus any representing matrix for B is a symmetric matrix.

If B is a symmetric form on V define $Q : V \to F$ via $Q(v) = B(v,v)$, and call Q the associated quadratic form. Note that

$$Q(av) = a^2 Q(v)$$

for all $a \in F$, all $v \in V$, and that

$$Q(u+v) = B(u+v, u+v) = Q(u) + 2B(u,v) + Q(v)$$

for all $u, v \in V$. Thus

$$B(u,v) = \frac{1}{2}[Q(u+v) - Q(u) - Q(v)],$$

and the bilinear form B is completely determined by the quadratic form Q.

If $\{v_1, v_2, \ldots, v_n\}$ is a basis for V, and $\widehat{B} = [b_{ij}]$, as usual, and $v \in V$, write $v = \sum_i a_i v_i$. Then

$$Q(v) = B(v,v) = \sum_{i,j} b_{ij} a_i a_j,$$

so Q is a homogeneous degree 2 polynomial function in the n coordinates of V relative to the basis. That is, in fact, the usual definition of a quadratic form.

Proposition 5.0.1. *If B is a nonzero symmetric bilinear form on V, with quadratic form Q, then $Q(v) \neq 0$ for some $v \in V$.*

Proof. If $Q(u) = 0$ for all u, then

$$0 = Q(u+v) = Q(u) + 2B(u,v) + Q(v) = 2B(u,v),$$

so $B(u,v) = 0$ for all $u, v \in V$, a contradiction. □

A set $\{v_1, \ldots, v_k\}$ of vectors in V is called orthogonal (relative to B) if $v_i \perp v_j$ (i.e., $B(v_i, v_j) = 0$) for $i \neq j$.

Theorem 5.0.2. *If B is a symmetric bilinear form on V then V has an orthogonal basis $\{v_1, \ldots, v_n\}$, relative to which B has diagonal representing matrix*

$$\widehat{B} = \begin{bmatrix} b_1 & 0 & & \\ 0 & \ddots & & 0 \\ & & b_r & \\ & & 0 & 0 \end{bmatrix},$$

with all $b_i \neq 0$, $r = rank(B)$, and $\{v_{r+1}, \ldots, v_n\}$ a basis for $rad(V)$.

Theorem 5.0.3. *Suppose F is a field in which every element has a square root (e.g., F algebraically closed). Then symmetric bilinear forms B_1 and B_2 on spaces V_1 and V_2 of the same dimension are equivalent if and only if B_1 and B_2 have the same rank.*

Proof. By Theorem 4.2 and the Notes following it any such form of rank r can be represented by the matrix $\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$, where I is an $r \times r$ identity matrix. Apply Proposition 2.8 of the text. □

Theorem 5.0.4 (Sylvester's Law of Inertia)**.** *Suppose F is an ordered field (e.g., $F \subseteq \mathbb{R}$), B is a symmetric bilinear form on a vector space V over F, and $\{u_1, \ldots, u_n\}, \{v_1, \ldots, v_n\}$ are orthogonal bases for V for which the matrices representing B are, respectively,*

$$\begin{bmatrix} b_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & b_p & & & & & & \\ & & & -b_{p+1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & -b_r & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix}, \begin{bmatrix} c_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & c_q & & & & & & \\ & & & -c_{q+1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & -c_r & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix},$$

with all $b_i, c_j > 0$, then $p = q$.

Sir has also emphasized thar Sylvester's Law of Inertia plays a crucial role in physics, especially in mechanics and relativity, by classifying quadratic forms like energy or space-time intervals. It ensures that under coordinate transformations, the number of positive, negative, and zero eigenvalues of a symmetric matrix remains invariant, preserving physical properties like causality and stability.

For the later theorems, one can draw parallels to results from Chapter 3 and section 3.6 of Simeon Ball.

Chapter 6

Orthogonal Geometry (Char $\neq$2)

Orthogonal Transformations in Quadratic Spaces

Let V be a quadratic space over a field F with $\text{char}(F) \neq 2$. The **orthogonal group** $O(V)$ consists of linear transformations that preserve the bilinear form B (or equivalently the quadratic form Q):

$$O(V) = \{\tau \in \text{GL}(V) : B(\tau u, \tau v) = B(u, v)\ \forall u, v \in V\}$$

Equivalently, $\tau \in O(V) \iff Q(\tau v) = Q(v)\ \forall v \in V$. Using a basis, $\tau \in O(V)$ if and only if:

$$T^T \widehat{B} T = \widehat{B}, \quad \text{implying } \det(T) = \pm 1.$$

- $\det(\tau) = 1$: *proper* orthogonal transformation (rotation)
- $\det(\tau) = -1$: *improper* orthogonal transformation (reversion)

The subgroup of all proper orthogonal transformations is the **special orthogonal group** $\text{SO}(V)$, satisfying:

$$[O(V) : \text{SO}(V)] = 2.$$

Recall,Suppose that B is a reflexive bilinear form on V, and that W is a nondegenerate subspace of V. Then $V = W \oplus W^{\perp}$.

Let $u \in V$ be any nonzero anisotropic vector (i.e., $Q(u) \neq 0$), and define a linear transformation σ_u via

$$\sigma_u(v) = v - 2\frac{B(v,u)}{Q(u)} \cdot u$$

for all $v \in V$. Then

$$\begin{aligned} B(\sigma_u v, \sigma_u w) &= B\left(v - 2\frac{B(v,u)}{Q(u)}u, w - 2\frac{B(w,u)}{Q(u)}u\right) \\ &= B(v,w) - 4\frac{B(v,u)B(w,u)}{Q(u)} + 4\frac{B(v,u)B(w,u)Q(u)}{Q(u)^2} \\ &= B(v,w), \end{aligned}$$

so $\sigma_u \in O(V)$.

Note that $\sigma(u) = -u$, and if $v \perp u$ then $\sigma_u v = v$. We call σ_u the (orthogonal) reflection along u or through the hyperplane $u^\perp$. Often in the literature σ_u is called a symmetry.

Since $Q(u) \neq 0$ we have $V = \langle u \rangle \oplus \langle u \rangle^\perp$ by Proposition 2.9. If we set $u_1 = u$ and choose any basis $\{u_2, \ldots, u_n\}$ for $\langle u \rangle^\perp$, the relative to the basis $\{u_1, u_2, \ldots, u_n\}$ for V the matrix representing σ_u is

$$\begin{bmatrix} -1 & 0 \\ 0 & I_{n-1} \end{bmatrix},$$

so σ_u is improper. Clearly σ_u is of order 2.

Witt's Cancellation Theorem

Theorem 6.0.1. *Suppose that U_1 and U_2 are nondegenerate subspaces of a quadratic space V, and $\sigma : U_1 \to U_2$ is an isometry. Then $U_1^\perp$ and $U_2^\perp$ are also isometric.*

Proof. We proceed by induction on the dimension of U_1. First, consider the base case where $\dim U_1 = 1$. Suppose $U_1 = \langle u_1 \rangle$ and $U_2 = \langle u_2 \rangle$. Since U_1 and U_2 are nondegenerate, we have $Q(u_1) \neq 0$ and $Q(u_2) \neq 0$. Because $\sigma : U_1 \to U_2$ is an isometry, $\sigma(u_1) = cu_2$ for some $c \in F$, and $Q(\sigma(u_1)) = Q(u_1)$, so $Q(cu_2) = c^2 Q(u_2) = Q(u_1)$. Without loss of generality, we may adjust the scalar and assume $\sigma(u_1) = u_2$, which implies $Q(u_1) = Q(u_2)$. Let $Q(u_1) = Q(u_2) = a \neq 0$.

To proceed, compute $Q(u_1+u_2) = B(u_1+u_2, u_1+u_2) = Q(u_1)+2B(u_1, u_2)+Q(u_2) = 2a+2B(u_1, u_2)$, since $B(u_1, u_2) = B(u_2, u_1)$. Similarly, $Q(u_1-u_2) = Q(u_1)-2B(u_1, u_2)+Q(u_2) = 2a-2B(u_1, u_2)$. If both were zero, then $2a+2B(u_1, u_2) = 0 \implies B(u_1, u_2) = -a$, and $2a - 2B(u_1, u_2) = 0 \implies B(u_1, u_2) = a$, so $a = -a$. Since char $F \neq 2$, this implies $2a = 0$, hence $a = 0$, contradicting $Q(u_1) \neq 0$. Thus, at least one of $Q(u_1 + u_2)$ or $Q(u_1 - u_2)$ is nonzero.

Without loss of generality, assume $Q(u_1+u_2) \neq 0$. (The case $Q(u_1-u_2) \neq 0$ is similar, using $\sigma_{u_1-u_2}$.) Compute the orthogonality: $B(u_1 + u_2, u_1 - u_2) = Q(u_1) - B(u_1, u_2) + B(u_2, u_1) - Q(u_2) = a - B(u_1, u_2) + B(u_1, u_2) - a = 0$, so $u_1 - u_2 \perp u_1 + u_2$. Now apply the reflection $\sigma_{u_1+u_2}$, defined as $\sigma_{u_1+u_2}(v) = v - 2\frac{B(v,u_1+u_2)}{Q(u_1+u_2)}(u_1+u_2)$. Since $B(u_1-u_2, u_1+u_2) = 0$, we have $\sigma_{u_1+u_2}(u_1 - u_2) = u_1 - u_2$. Next, express $u_1 = \frac{1}{2}(u_1 + u_2) + \frac{1}{2}(u_1 - u_2)$. Then $\sigma_{u_1+u_2}(u_1) = \sigma_{u_1+u_2}\left(\frac{1}{2}(u_1 + u_2) + \frac{1}{2}(u_1 - u_2)\right) = \frac{1}{2}\sigma_{u_1+u_2}(u_1 + u_2) + \frac{1}{2}\sigma_{u_1+u_2}(u_1 - u_2) = \frac{1}{2}(-(u_1 + u_2)) + \frac{1}{2}(u_1 - u_2) = \frac{1}{2}(-u_1 - u_2 + u_1 - u_2) = -u_2$.

Since $\sigma_{u_1+u_2} \in O(V)$, it preserves orthogonality. For $v \in u_1^\perp$, $B(v, u_1) = 0$. Compute $B(\sigma_{u_1+u_2}(v), u_2) = B(v, \sigma_{u_1+u_2}(u_2))$. Note $u_2 = \frac{1}{2}(u_1 + u_2) - \frac{1}{2}(u_1 - u_2)$, so $\sigma_{u_1+u_2}(u_2) = \frac{1}{2}(-(u_1 + u_2)) - \frac{1}{2}(u_1 - u_2) = -u_1$. Thus, $B(\sigma_{u_1+u_2}(v), u_2) = B(v, -u_1) = -B(v, u_1) = 0$, so $\sigma_{u_1+u_2}(v) \in u_2^\perp$. Since $\dim u_1^\perp = \dim u_2^\perp$, we conclude $\sigma_{u_1+u_2}(u_1^\perp) = u_2^\perp$, and $U_1^\perp = u_1^\perp$ is isometric to $U_2^\perp = u_2^\perp$.

Now consider the inductive step where $\dim U_1 > 1$. Assume the theorem holds for subspaces of dimension less than $\dim U_1$. Choose an anisotropic vector $u_1 \in U_1$, so $Q(u_1) \neq 0$. Let W_1 be the orthogonal complement of $\langle u_1 \rangle$ in U_1, so $U_1 = \langle u_1 \rangle \oplus W_1$, and W_1 is nondegenerate by Proposition 2.9. Set $u_2 = \sigma(u_1)$, which is anisotropic, and $W_2 = \sigma(W_1)$, so $U_2 = \langle u_2 \rangle \oplus W_2$, with $W_2 \perp \langle u_2 \rangle$. We can decompose $V = \langle u_1 \rangle \oplus W_1 \oplus U_1^\perp = \langle u_2 \rangle \oplus W_2 \oplus U_2^\perp$. By the base case, there exists an isometry $\eta : W_1 \oplus U_1^\perp \to W_2 \oplus U_2^\perp$. Since $\dim W_1 = \dim U_1 - 1$, and $\sigma : W_1 \to W_2$ is an isometry, the inductive hypothesis implies $W_1^\perp = U_1^\perp$ is isometric to $W_2^\perp = U_2^\perp$. Thus, $U_1^\perp \cong U_2^\perp$.

By induction, the theorem holds for all dimensions of U_1. This completes the proof. □

Recall,

Proposition 6.0.2. *Suppose that V is a quadratic space and that U is a subspace with $\text{rad}U \neq 0$. Let U' be any complementary subspace for $\text{rad}U$ in U, i.e., $U = \text{rad}U \oplus U'$. If $\{u_1, \ldots, u_k\}$ is a basis for $\text{rad}U$ then there is a subspace W, with basis $\{v_1, \ldots, v_k\}$, such that $U \cap W = 0$, $U \oplus W$ is nondegenerate, (u_i, v_i) is a hyperbolic pair for $H_i = \langle u_i, v_i \rangle$, $1 \leq i \leq k$, and*

$$U \oplus W = U' \oplus H_1 \oplus H_2 \oplus \cdots \oplus H_k.$$

Witt's Extension Theorem

Theorem 6.0.3 (Witt's Extension Theorem)**.** *Let (V, q) be a quadratic space, and let $U_1, U_2 \subseteq V$ be subspaces. If $\sigma : U_1 \to U_2$ is an isometry, then there exists $\tau \in O(V)$ such that $\tau|_{U_1} = \sigma$.*

Proof. The proof is divided into two cases.

Case 1: Nondegenerate Subspaces

Assume U_1 and U_2 are nondegenerate. By Witt's Cancellation Theorem, there exists $\eta : U_1^\perp \to U_2^\perp$ an isometry. Since $V = U_1 \oplus U_1^\perp$, define $\tau(u + w) = \sigma(u) + \eta(w)$, which is an isometry and $\tau|_{U_1} = \sigma$.

Case 2: Degenerate Subspaces

Assume U_1 is degenerate, i.e., $\text{rad } U_1 \neq \{0\}$. Decompose $U_1 = \text{rad } U_1 \oplus U_1'$. By Proposition 6.0.2, find W_1 such that $U_1 \oplus W_1 = U_1' \oplus H_1 \oplus \cdots \oplus H_k$, where each H_i is a hyperbolic plane. Extend σ to $\sigma' : U_1 \oplus W_1 \to U_2 \oplus W_2$, and apply Case 1 to find τ with $\tau|_{U_1} = \sigma$. □

Chapter 7

Field theory and Coding Theory

Topics Covered

Here, I am including all the important results from the field theory that might be useful. Normally, a person who has taken a course in Fields and Galois Theory can skip this section since they will be familiar with the content in this chapter. We assume knowledge of polynomial rings to understand this material. Getting a flavor of the theorems is enough, but the proofs of some important theorems are included. The reader should be familiar with the notions of groups, rings, ideals, fields, quotient rings, isomorphisms of rings/fields, and field extensions.

Standard references are Chapter 15 of Michael Artin and Chapter 13 of Dummit and Foote.

Finite Fields

The simplest example of a finite field is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, that is, the integers modulo p, for a prime number p. The key property is that every non-zero element has a multiplicative inverse, which follows from Euclid's theorem: for any integers a, b with $\gcd(a, b) = 1$, there exist integers x and y such that $ax + by = 1$.

A finite field is a field with finitely many elements. An important result is the structure theorem for finite fields.

Important

Finite Fields

Theorem 7.0.1. *For every finite field F, there exists a prime number p and a positive integer n such that $|F| = p^n$.*

Proof. Let p be the characteristic of F, and let n be the dimension of F as a vector space over its prime subfield $\mathbb{F}_p$. Then the number of elements in F is p^n. □

Theorem 7.0.2. *For every prime power q, there exists a unique (up to isomorphism) finite field of order q.*

Proof. Let $q = p^n$ where p is prime. Every finite field of characteristic p is algebraic over $\mathbb{F}_p$ and hence lies in an algebraic closure $\overline{\mathbb{F}_p}$. The unique field of order q is the set of roots of the polynomial $x^q - x$ in $\overline{\mathbb{F}_p}$. This field is denoted by $\mathbb{F}_q$. □

Construction: The most concrete way to construct $\mathbb{F}_q$ is to choose an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n (which always exists), and then define

$$\mathbb{F}_q = \mathbb{F}_p[x]/(f(x)).$$

Basic Properties of $\mathbb{F}_q$

(a) For every $\alpha \in \mathbb{F}_q$, we have $\alpha^q = \alpha$. The elements of the prime subfield are precisely the roots of $x^p - x \in \mathbb{F}_q[x]$.

(b) $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m \mid n$. Moreover, for each divisor m of n, there exists a unique copy of $\mathbb{F}_{p^m}$ inside $\mathbb{F}_{p^n}$, consisting of all $\alpha \in \mathbb{F}_{p^n}$ satisfying $\alpha^{p^m} = \alpha$.

(c) The additive group of $\mathbb{F}_q$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$, and hence isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$. Any generator is called a **primitive element**.

(d) The map $x \mapsto x^p$ is an automorphism of $\mathbb{F}_q$. The full automorphism group of $\mathbb{F}_q$ is cyclic of order n, consisting of maps $x \mapsto x^{p^i}$ for $i = 1, \ldots, n$.

(e) If q is odd, then $\mathbb{F}_q^\times$ has exactly $(q-1)/2$ squares (quadratic residues) and $(q-1)/2$ non-squares. Multiplying by a square preserves the sets; multiplying by a non-square swaps them. If q is even, every element in $\mathbb{F}_q$ is a square since $x \mapsto x^2$ is an automorphism.

Theorem 7.0.3. *For all $i \in \mathbb{N}$, $i \neq 0$, we have*

$$\sum_{a \in \mathbb{F}_q} a^i = \begin{cases} -1 & \text{if } i \equiv 0 \mod (q-1), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $S = \sum_{a \in \mathbb{F}_q} a^i$ and let α be a generator of the multiplicative group $\mathbb{F}_q^\times$. Then:

$$S = \sum_{a \in \mathbb{F}_q} a^i = \sum_{a \in \mathbb{F}_q^\times} a^i + 0 = \sum_{j=0}^{q-2} \alpha^{ij}.$$

This is a geometric sum. If $i \not\equiv 0 \mod (q-1)$, then $\sum_{j=0}^{q-2} \alpha^{ij} = 0$. If $i \equiv 0 \mod (q-1)$, then each term is 1, giving $q-1$. So the total sum is:

$$S = (q-1) + 0 = -1 \quad \text{(in characteristic } p\text{)}.$$

□

[0] In finite geometry literature, the field $\mathbb{F}_q$ is sometimes denoted by $GF(q)$ (Galois Field).

Trace and Norm Functions

Let $\mathbb{F}_{q^n}$ be a field extension of $\mathbb{F}_q$. Then:

Definition 7.0.4. The **trace function** $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is defined as

$$\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

The **norm function** $\mathrm{Norm} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ is defined as

$$\mathrm{Norm}(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{n-1}} = x^{(q^n-1)/(q-1)}.$$

If $\mathbb{F}_q$ is the prime subfield, these are known as the **absolute trace** and **absolute norm**.

Theorem 7.0.5. *The trace function* $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *is an additive and surjective function. For all* $a \in \mathbb{F}_q$*, the preimage* $\mathrm{Tr}^{-1}(a)$ *has size* q^{n-1}*.*

Theorem 7.0.6. *The norm function* $\mathrm{Norm} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ *is multiplicative. For all* $a \in \mathbb{F}_q^\times$*, we have* $|\mathrm{Norm}^{-1}(a)| = \frac{q^n-1}{q-1}$*.*

Coding Theory

The following mostly follows chapters 1-4 of [3] and you can watch the following talk: *What is Coding Theory?* by Prof. Krishna Kaipa (Maths Club Talk Series Episode 2 - IISER Pune).

7.1 Introduction

Coding theory is a mathematical framework for designing reliable communication over noisy channels. The primary goal is to encode messages so that errors introduced during transmission can be detected and corrected.

A communication system consists of:

- A source generating messages.
- An encoder mapping messages to codewords.
- A noisy channel causing errors.
- A decoder reconstructing the original message.

The core challenge is balancing redundancy with efficiency, ensuring reliable transmission while maximizing the data rate. The redundancy introduced by the encoding process enables error detection and correction, which is fundamental in many real-world applications like satellite communication, deep-space transmission, and data storage systems.

7.2 Fundamentals of Coding Theory

7.2.1 Hamming Distance and Error Correction

The Hamming distance between two codewords x and y is defined as:

$$d_H(x, y) = \sum_{i=1}^{n} \mathbf{1}(x_i \neq y_i). \tag{7.2.1}$$

This measures the number of differing positions between two strings of equal length.

The minimum distance of a code is:

$$d_{\min} = \min_{x \neq y} d_H(x, y). \tag{7.2.2}$$

A code can detect up to $d_{\min} - 1$ errors and correct up to $t = \lfloor (d_{\min} - 1)/2 \rfloor$ errors. The larger the minimum distance, the stronger the error-correcting capability of the code.

7.2.2 Linear Codes and Generator Matrices

A linear code C of length n and dimension k over a field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. It is defined by a generator matrix G:

$$C = \{uG \mid u \in \mathbb{F}_q^k\}. \tag{7.2.3}$$

The parity-check matrix H satisfies:

$$Hx^T = 0 \quad \forall x \in C. \tag{7.2.4}$$

Syndrome decoding utilizes H to detect and correct errors. Examples of linear codes include Hamming codes, BCH codes, and Reed-Solomon codes, each serving different purposes in digital communication and data storage.

7.3 Important Bounds in Coding Theory

7.3.1 Singleton Bound

For a code with parameters (n, k, d),

$$d \leq n - k + 1. \tag{7.3.1}$$

This upper bounds the error-correcting capacity. Codes that achieve this bound are called maximum distance separable (MDS) codes.

7.3.2 Hamming Bound

The Hamming bound states:

$$q^n \geq \sum_{i=0}^{t} \binom{n}{i} (q-1)^i q^k. \tag{7.3.2}$$

This ensures codes do not exceed sphere-packing limits, restricting the number of possible codewords in a given space.

Quotient Spaces

Let U be a subspace of $V_k(\mathbb{F})$. For all $v \in V_k(\mathbb{F})$, the set

$$v + U = \{u + v \mid u \in U\}$$

is a *coset* of U. The set of cosets

$$V_k(\mathbb{F})/U = \{v + U \mid v \in V_k(\mathbb{F})\}$$

forms a vector space over $\mathbb{F}$ called the *quotient space*, where we define

$$\lambda(v + U) = \lambda v + U$$

for all $\lambda \in \mathbb{F}$ and $v \in V_k(\mathbb{F})$, and

$$v + U + w + U = v + w + U,$$

for all $v, w \in V_k(\mathbb{F})$.
Result: *The dimension of* $V_k(\mathbb{F})/U$ *is* $k - \dim U$.

The Quotient Topology

We have used the notion of quotient topology multiple times while reading. Since this was not included in my topology course, I am including it here. A standard reference for this would be Section 22 of Chapter 2 of Topology by Munkres.

Definition 7.3.1 (Quotient Space)**.** Let X be a topological space, and let $\sim$ be an equivalence relation on X. The set of equivalence classes under $\sim$ is denoted by $X^* = X/\sim$.

The quotient topology on X^* is defined as follows: a subset $U \subseteq X^*$ is open if and only if its preimage $p^{-1}(U)$ under the natural projection map $p : X \to X^*$ is open in X.

The space X^* equipped with this topology is called the quotient space of X. It is also known as the identification space or decomposition space.

Group Action

A **group action** of a group G on a set X is a function $\phi : G \times X \to X$ such that:

1. **Identity:** $e \cdot x = x$ for all $x \in X$.
2. **Compatibility:** $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

A group action allows us to study symmetries and partition X into orbits.

Orbits and Stabilizers

The **orbit** of $x \in X$ is $\text{Orb}(x) = \{g \cdot x \mid g \in G\}$. The orbit represents all possible elements reachable from x under G's action.

The **stabilizer** of x is the subgroup $G_x = \{g \in G \mid g \cdot x = x\}$, which consists of elements in G that fix x.

Orbit-Stabilizer Theorem

For a finite group G acting on X,

$$|G| = |G_x| \cdot |\text{Orb}(x)|. \tag{7.3.3}$$

Proof: The function $\varphi : G/G_x \to \text{Orb}(x)$ given by $gG_x \mapsto g \cdot x$ is a bijection. Thus,

$$|\text{Orb}(x)| = |G : G_x| = \frac{|G|}{|G_x|}. \tag{7.3.4}$$

Multiplying by $|G_x|$ gives the result. This theorem relates the size of G to its action on X.

Bibliography

[1] Simeon Ball, *Finite Geometry and Combinatorial Applications*, London Mathematical Society Student Texts, Cambridge University Press, 2015. Available at: https://www.cambridge.org/us/universitypress/subjects/mathematics/discrete-mathematics-information-theory-and-coding/finite-geometry-and-combinatorial-applications

[2] Larry C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, Volume 39, American Mathematical Society, 2002. Available at: https://bookstore.ams.org/gsm-39/

[3] Raymond Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Clarendon Press, Oxford, 1986.

[4] Anurag Bishnoi, *Finite Geometry and Combinatorial Applications*, Lecture notes, 2019. Available at: https://discretemath.imp.fu-berlin.de/DMIII-2019/finite_geometry.pdf

[5] Keith Conrad, *Bilinear Forms*, Mathematics Department, University of Connecticut. Available at: https://kconrad.math.uconn.edu/blurbs/

[6] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd Edition, Wiley, 2004.

[7] Rey Casse, *Projective Geometry: An Introduction*, Oxford University Press, 2006. Available at: https://academic.oup.com/book/52911

[8] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd Edition, Oxford University Press, 1998. Available at: https://academic.oup.com/book/53387

[9] Gary L. Mullen and Carl Mummert, *Finite Fields and Applications*, Student Mathematical Library, Volume 41, American Mathematical Society, 2007. Available at: https://bookstore.ams.org/stml-41/

Sunil K. Chebolu, Dan McQuillan, and Ján Mináč, *Witt's Cancellation Theorem Seen as a Cancellation*,

Available at: https://www.math.uwo.ca/faculty/minac/wittcancellation.pdf

[10] Artin, E. (1957). *Geometric Algebra*.