1 Groups

Theorem 1.1 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. Then $|H|$ divides $|G|$.*

Theorem 1.2. *If H is a subgroup of G then for all $a, b \in G$ $|aH| = |bH|$ and either $aH = bH$ or $aH \cap bH = \emptyset$ (i.e. the cosets partition the group)*

Theorem 1.3 (Cayley's Theorem)**.** *Every finite group G is isomorphic to a subgroup of a permutation group. If G has order n then it is isomorphic to a subgroup of the symmetric group S_n.*

Theorem 1.4. *Let $(S, \circ)$ be a G-Set (i.e. $\circ$ is a G-action on S). If s in$S$ and H_s is the stabilizer of s while $O_s \subseteq S$ is the orbit of S then there is a bijection*

$$\varphi : G/H \to O_s$$

defined by $aH \to as$. Further $\varphi(gC) = g \circ \varphi(C)$ for every coset C and $g \in G$.

Corollary 1.5 (Counting Theorem)**.** *Let $(S, \circ)$ be a G-Set. If $s \in S$ then we have*
(order G) = (order of stabilizer of s)(order of orbit of s)

$$|G| = |H_s||O_s|$$

or equivalently $|O_s| = [G : H_s]$

Corollary 1.6. *$|S| = \sigma_i |O_i|$ where each orbit O_i occurs exactly once.*

Theorem 1.7. *Conjugation is a group action*

Lemma 1.8. *Let $|G| = p^e$. Then the center of G has order > 1*

1.1 Sylow's Theorems

Theorem 1.9 (1st Sylow Theorem)**.** *Let G be a finite group of order n ($|G| = n$) and let p be a prime such that*

- *$n = p^e \cdot m$*
- *p does not divide m*

then there is an element of G of order p^e.

Corollary 1.10. *IF p divides $|G|$ then G contains an element of order p.*

Theorem 1.11 (2nd Sylow Theorem)**.** *Let K be a subgroup of G with order divisible by p. Let H be a p-Sylow subgroup of G. Then there is a conjugacy subgroup of $H' = gHg^{-1}$ such that $K \cap H'$ is a Sylow p-subgroup of K*

Lemma 1.12. *Let $(S, \circ)$ be a G-Set and let $s \in S$. Let s' be in the ordit of s, say $s' = a \circ s$. Then*

$$G_{s'} = aG_s a^{-1}$$

Where $G_s, G_{s'}$ are the stabilizers of s, s' respectively.

Corollary 1.13. *The Sylow p-subgroups of a group are all conjugate and every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.*

Theorem 1.14 (3rd Sylow Theorem)**.** *Let $|G| = n = p^e m$ where p does not divide m. Let s be the number of p-Sylow subgroups of G. Then s divides m and $s = ap + 1$ for some integer a.*

1.2 Abelian Groups

Theorem 1.15. *Let A be an abelian group. Then $\{a \in A : (\exists n \in \mathbb{Z}) na = 0\}$ is a subgroup of A, called the Torsion Subgroup of A*

Recall that we say $F = \langle v_1, \cdots, v_n \rangle$ if every element of F can be expressed as a linear combination (over $\mathbb{Z}$) of $v_1, \ldots, v_n$ in a unique way. We can think of $\{v_1, \cdots, v_n\}$ as a "basis" for F over $\mathbb{Z}$.

Theorem 1.16. *Let F be a free abelian group of rank r and let G be a subgroup of F of rank $s \leq r$ (but $s > 0$). Then G is a free abelian group of rank $s \leq r$. Further F has a set of generators $\langle u_1, \cdots u_r \rangle$ such that G is generated by*

$$\begin{array}{ccccccccc} v_1 & = & a_{11}u_1 & + & a_{12}u_2 & + & \cdots & + & a_{1r}u_r \\ v_2 & = & & & a_{22}u_2 & + & \cdots & + & a_{2r}u_r \\ \vdots & & & & \vdots & & \cdots & & \vdots \\ v_s & = & & & a_{ss}u_s & + & \cdots & + & a_{sr}u_r \end{array}$$

for some a_{ij} such that all a_{ii} are positive

Theorem 1.17. *Let F be a finitely generated abelian group with a basis $\langle u_1, \cdots, u_r\rangle$. Let $v = b_1u_1 + \cdots + b_ru_r$ with $gcd(b_1, \cdots, b_r) = 1$. Then there exists $v_2, \cdots v_r$ such that $F = \langle v, v_2, \ldots, v_r\rangle$*

Theorem 1.18. *Let F be a finitely generated abelian group and let G be a subgroup of F. Then there are elements $v_1, \ldots v_r \in F$ such that*

$$F = \langle v_1, \ldots, v_r\rangle$$

$$G = \langle h_1v_1, \ldots, h_sv_r\rangle$$

where $h_1, \ldots h_r$ are all positive and h_i divides h_{i+1}.

Theorem 1.19 (Unique Decomposition of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group A can be expressed as the direct sum of cyclic groups*

$$A \cong \mathbb{Z}^m \oplus \mathbb{Z}/(h_1) \oplus \mathbb{Z}/(h_2) \ldots \mathbb{Z}/(h_j)$$

where h_i divides h_{i+1}. Further, this decomposition is unique.

Theorem 1.20. *Let A be a finite Abelian group with $|A| = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n}$. Further let P_i be the collection of all elements of A of order a power of P_i. Then*

$$A = P_1 \oplus P_2 \oplus \cdots \oplus P_n$$

Corollary 1.21. *Let $e = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n}$. Then*

$$\mathbb{Z}/(e) \cong \mathbb{Z}/(p_1^{a_1}) \oplus \cdots \oplus \mathbb{Z}/(p_n^{a_n})$$

Lemma 1.22. *Let G be any group. Suppose $x, y \in G$ and $xy = yx$ and the order of x is relatively prime to the order of y. Then $\langle x, y\rangle = \langle xy\rangle$*

2 Vector Spaces

Theorem 2.1. *Let V be a finite dimensional vector space over a field F and let $\langle , \rangle$ be a bilinear form on V. If B is a basis for V then there is a matrix A such that $\langle v, w\rangle = v_B^t A w_B$ where v_B, w_B are the matirx representations of v, w with respect to the basis B*

Theorem 2.2. *Let V be a finite dimensional vector space over a field F and let B is a basis for V. Then the map $\langle v, w\rangle = v_B^t A w_B$ is a bilinear form for every matirx A (where v_B, w_B are as in the previous theorem)*

Lets now deal with Real Vector Spaces

Theorem 2.3. *Let A be the matrix associated to a bilinear form $\langle , \rangle$ on V relative to a basis B. Then those matrixes which represent the same form relative to different basis are those matrixes of the form*

$$QAQ^t$$

for some $Q \in GL_n(F)$.

Lemma 2.4. *If you change basis by an orthogonal change of base (i.e. the change of base matrix is orthogonal) then the dot product is preserved.*

Lemma 2.5. *The matrixes which represent the dot product under some basis are those of the form PP^t for $P \in GL_n(\mathbb{R})$.*

Lemma 2.6. *A bilinear form is symmetric if and only if the matrix associated to it is symmetric.*

Lemma 2.7. *Let B be an orthonormal basis for V relative to $\langle , \rangle$. Then the matrix associated to $\langle , \rangle$ under B is the identity matrix.*

Theorem 2.8 (Gram-Schmidt)**.** *Let $\langle , \rangle$ be a positive definite symmetric bilinear form on a finite dimensional vector space V. Then there is an orthonormal basis for V*

Theorem 2.9. *The following are equivalent*

- *A represents the dot product*
- *There is a $P \in GL_n(\mathbb{R})$ such that $A = PP^t$*
- *A is symmetric and positive definite.*

Theorem 2.10. *Let $V, \langle , \rangle$ be a Euclidean space (where $|v| = \sqrt{\langle v, v\rangle}$). Then we have the Schwartz inequality$|\langle v, w\rangle| \leq |v| \cdot |w|$*
$|v + w| \leq |v| + |w|$

Lemma 2.11. *Let V be a vector space and let $\langle , \rangle$ be a bilinear form on V. If $W \subseteq V$ is a subspace then $\langle , \rangle$ restricts to a bilinear form $\langle , \rangle|_W$ on W. Further if $\langle , \rangle$ is positive definite or symmetric so is $\langle , \rangle|_W$*

Lemma 2.12. *Let $\langle , \rangle$ be a non-identically zero symmetric bilinear form on V. Then there is a $v \in V$ such that $\langle v, v \rangle \neq 0$.*

Theorem 2.13. *Let $\langle , \rangle$ be a symmetric bilinear form on V (a finite dimensional vector space). If $W \subseteq V$ is a subspace such that $\langle , \rangle|_W$, the bilinear form restricted to W, is non-degenerate, then*

$$V = W \oplus W^{\perp}$$

Theorem 2.14. *Let $\langle , \rangle$ be a symmetric bilinear form on V (a finite dimensional vector space). Then there is an orthogonal basis for V.*

Theorem 2.15 (Sylvester's Law)**.** *The signature of a symmetric bilinear form on a finite dimensional vector space is independent of the basis.*

Theorem 2.16. *Let $\langle w_1, \ldots, w_r \rangle$ be an orthonormal basis for $W \subseteq V$ (relative to a bilinear form $\langle , \rangle$). Then the orthogonal projection $\pi_W(v)$ of v onto W is the vector*

$$\pi_W(v) = \langle v, w_1 \rangle w_1 + \cdots + \langle v, w_n \rangle w_n$$

Corollary 2.17. *Let $\langle v_1, \ldots, v_n \rangle$ be an orthonormal basis for V (relative to a bilinear form $\langle , \rangle$). Then*

$$(\forall v \in V) v = \langle v, v_1 \rangle v_1 + \cdots \langle v, v_n \rangle, v_n$$

2.1 Hermitian Forms

Theorem 2.18. *Let V be a finite dimensional complex vector space and let $\langle , \rangle$ be a hermitian form on V. If B is a basis for V then there is a hermitian matrix A such that $\langle v, w \rangle = v_B^* A w_B$ where v_B, w_B are the matirx representations of v, w with respect to the basis B*

Theorem 2.19. *Let V be a finite dimensional complex vector space and let B is a basis for V. Then the map $\langle v, w \rangle = v_B^t A w_B$ is a hermitian form for every hermitian matirx A (where v_B, w_B are as in the previous theorem)*

Lemma 2.20. *If A, B are complex $n \times n$ matrixes then*

$$(A+B)^* = A^* + B^*$$

$$(AB)^* = B^*A^*$$

$$(A^*)^{-1} = (A^{-1})^*$$

$$A^{**} = A$$

Theorem 2.21. *Let A be the matrix associated to a hermitian form $\langle , \rangle$ on V relative to a basis B. Then those matrixes which represent the same form relative to different basis are those matrixes of the form*

$$QAQ^*$$

for some $Q \in GL_n(\mathcal{C})$.

Lemma 2.22. *The unitary matrixes form a group.*

Lemma 2.23. *A change of base preserves the standard hermitian dot product if and only if the change of base is unitary.*

Theorem 2.24 (Spectral Theorem)**.**

(a) Let T be a hermitian operator on a hermitian vector space V. Then there is an orthonormal basis for V consisting of eigenvectors of T.

(b) Let M be a hermitian matrix. Then there are unitary matrixes such that PMP^* is a real diagonal matrix

Corollary 2.25. *The eigenvalues of a hermitian operator are real.*

Lemma 2.26. *If M is normal and P is unitary then $M' = PMP^*$ is normal.*

Theorem 2.27 (Spectral Theorem for Normal Operators)**.** *A complex matrix M is normal if and only if there is a unitary matrix P such that PMP^* is diagonal.*

3 Rings

Theorem 3.1 (Substitution Principle)**.** *Let $\varphi : R \to R'$ be a ring homomorphism*

(a) Given an element $\alpha \in R'$ there is a unique homomorphism $\Phi : R[x] \to R'$ which agrees with the map φ on constant polynomials and sends $x \to \alpha$.

(b) Given elements $\alpha_1, \cdots, \alpha_n \in R'$ there is a unique ring homomorphism $\Phi : R[x_1, \ldots, x_n]$ such that $\Phi|_R = \phi$ and $\Phi[x_i] = \alpha_i$.

Lemma 3.2. *For every ring R there is a unique ring homomorphism $\mathbb{Z} \to R$.*

Lemma 3.3. *If R is a ring and $a \in R$ then $\{ra : r \in R\} = (a)$ is an ideal.*

Theorem 3.4. *A ring R is a field if and only if it has exactly two ideals.*

Corollary 3.5. *Let F be a field and R a non-zero ring. Then every homomorphism $\varphi : F \to R$ is injective.*

Lemma 3.6. *Every ideal in $\mathbb{Z}$ is principle.*

Theorem 3.7. *Let $g(x)$ be a monic polynomial in $R[x]$ and let α be an element of R such that $g(\alpha) = 0$. Then $x - \alpha$ divides $g(x)$.*

Theorem 3.8. *If F is a field then every ideal of $F[x]$ is principle.*

Corollary 3.9. *Let F be a field and let $f, g \in F[x]$ which are both non-zero. Then there is a unique monic $d(x) \in F[x]$ called the greatest common divisor of f, g such that*

(a) d generates the ideal (f, g) of $F[x]$ generated by f, g.

(b) d divides f and g

(c) If h is any divisor of f and g then h divides d.

(d) There are $p, q \in F[x]$ such that $d = pf + qg$