The Final Exam is in our usual classroom (B203 Van Vleck) at 7:25pm on Saturday May 13. It consists of approximately six proofs from the material below which I will write on the blackboard.

A copy of this document will be handed out to you at the Final.

# 1 Review

**Theorem 1.1** *Minimal polynomials are irreducible: If $\alpha$ is in some extension field of $F$ and define:*

$$I = \{f(x) \in F[x] : f(\alpha) = 0\}$$

*Then:*

*(a) $I$ is an ideal in $F[x]$*

*(b) (assuming $I$ is nontrivial) $I = \langle p(x) \rangle$ where $p(x)$ is any polynomial of minimal positive degree in $I$ and*

*(c) $p(x)$ is irreducible and so $I$ is a maximal ideal.*

**Theorem 1.2** *If $p(x)$ is an irreducible polynomial of degree $n$ in $F[x]$ and $\alpha$ a root of $p$ in some extension field, then $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis for $F(\alpha)$ as a vector space over $F$ and hence $[F(\alpha) : F] = n$.*

**Theorem 1.3** *Suppose char(F)=0 and $p(x) \in F[x]$ is irreducible, then $p$ does not have any multiple roots in any extension of $F$.*

**Theorem 1.4** *Suppose char(F)=0 and $[E : F] < \infty$, then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

**Theorem 1.5** *If $p(x) \in F[x]$ is an irreducible polynomial and $\alpha$ and $\beta$ are two roots of $p$, then $F(\alpha) \simeq F(\beta)$ with an isomorphism which fixes $F$ and takes $\alpha$ to $\beta$.*

**Theorem 1.6** *If $\sigma : F \to F'$ is an isomorphism, $f \in F[x]$ any polynomial, $E \supseteq F$ a splitting field of $f$ over $F$, and $E' \supseteq F'$ a splitting field of $\sigma(f)$ over $F'$, then there exists an isomorphism $\rho \supseteq \sigma$ such that $\rho : E \to E'$.*

# 2 Galois Theory

In this section we assume that all fields have characteristic 0.

**Definition 2.1** *The field $K \supseteq F$ is a Galois extension of the field $F$ iff $K$ is the splitting field over $F$ of some polynomial with coefficients in $F$.*

**Proposition 2.2** *Suppose $F \subseteq E \subseteq K$ are fields and $K$ is a Galois extension of $F$. Then $K$ is a Galois extension of $E$.*

**Definition 2.3** *For fields $F \subseteq E$ define* $\text{aut}(E|F)$ *to be the set of all automorphisms $\sigma$ of $E$ which fix $F$, i.e., $\sigma(a) = a$ for all $a \in F$.*

**Proposition 2.4** $\text{aut}(E|F)$ *is a group. Furthermore, if $F \subseteq E \subseteq K$ are fields, then* $\text{aut}(K|E)$ *is a subgroup of* $\text{aut}(K|F)$.

**Lemma 2.5** *Suppose $\sigma, \rho \in \text{aut}(F(\alpha)|F)$. Then $\sigma = \rho$ iff $\sigma(\alpha) = \rho(\alpha)$.*

*Similarly, if $\sigma, \rho \in \text{aut}(F(\alpha_1, \alpha_2, \ldots, \alpha_n)|F)$ then $\sigma = \rho$ iff $\sigma(\alpha_k) = \rho(\alpha_k)$ for all $k = 1, 2, \ldots, n$.*

**Theorem 2.6** *Suppose that $K$ is the splitting field of a polynomial in $F[x]$ of degree $n$. Then* $\text{aut}(K|F)$ *is isomorphic to a subgroup of $S_n$.*

**Lemma 2.7** *Suppose $K$ is a Galois extension of $F$, $K \subseteq L$, and $\sigma : K \to L$ an embedding which fixes $F$. Then and $\sigma(K) = K$.*

**Theorem 2.8** *Suppose $K$ is a Galois extension of $F$, then* $|\text{aut}(K|F)| = [K : F]$

**Lemma 2.9** *Suppose $F \subseteq E, E' \subseteq K$, $K$ is a Galois extension of $F$ and $\sigma : E \to E'$ and isomorphism which fixes $F$. Then there exists $\rho \in \text{aut}(K|F)$ which extends $\sigma$.*

**Theorem 2.10** *Suppose $K$ and $E$ are Galois extensions of $F$ and $F \subseteq E \subseteq K$. Then* $\text{aut}(K|E)$ *is a normal subgroup of* $\text{aut}(K|F)$ *and*

$$\frac{\text{aut}(K|F)}{\text{aut}(K|E)} \simeq \text{aut}(E|F)$$

# 3 Solvability by radicals

In this section we assume all our fields are subfields of the complex numbers $\mathbb{C}$.

**Definition 3.1** *For $G$ a finite group define $G$ is a solvable group by induction on $|G|$. $G$ is solvable iff either $G$ is abelian or there exists a normal subgroup $H \triangleleft G$ such that both $H$ and $G/H$ are solvable.*

**Definition 3.2** *Given fields $F \subseteq E \subseteq \mathbb{C}$ we say that $E$ is a radical Galois extension of $F$ iff there exists $n \in \mathbb{N}$ and $a \in F$ such that $E$ is the splitting field of the polynomial $x^n - a$ over $F$.*

**Theorem 3.3** *Suppose that $E$ is a radical Galois extension of $F$, then* $\text{aut}(E|F)$ *is a solvable group.*

**Lemma 3.4** *Suppose that $G$ is solvable group and $G'$ is a homomorphic image of $G$, then $G'$ is solvable. Hence quotient groups of solvable groups are solvable.*

**Theorem 3.5** *Suppose that $F_1 \subseteq F_2 \subseteq F_3 \cdots \subseteq F_m$ is a sequence of radical Galois extensions, i.e., $F_{k+1}$ is a radical Galois extension of $F_k$ for each $k = 1, 2, \ldots, m-1$. Suppose that $K$ is a Galois extension of $F_1$ such that $K \subseteq F_m$. Then $\mathrm{aut}(K|F_1)$ is a solvable group.*

**Corollary 3.6** *Suppose $f \in \mathbb{Q}[x]$ is a polynomial which is solvable by radicals. Then if $K$ is the splitting field of $f$ over $\mathbb{Q}$, then $\mathrm{aut}(K|\mathbb{Q})$ is a solvable group.*

**Theorem 3.7** *The group $A_5$ is simple.*

**Corollary 3.8** *The group $S_5$ is not solvable.*

**Lemma 3.9** *Suppose $G$ is a subgroup of $S_5$ which contains a transposition and a 5-cycle. Then $G = S_5$.*

**Example 3.10** *There is a polynomial $f \in \mathbb{Q}[x]$ of degree 5 whose splitting field $K$ has $\mathrm{aut}(K|\mathbb{Q})$ isomorphic to $S_5$, i.e., the Galois group of $f$ is $S_5$.*

**Corollary 3.11** *(Abel) Fifth degree polynomials are not solvable by radicals.*

# 4 Sylow Theorems

Let $p$ be a prime and $G$ a finite group.

**Definition 4.1** *Define group action $T : G \times X \to X$, $orb(x)$, $stab(x)$, $[G : H]$, $Z(G)$, $C(a)$, $conj(a)$, $p$-group, $p$-Sylow subgroup, $N(H)$.*

**Proposition 4.2** *If $G$ is group acting on a set $X$, then $stab(x)$ is a subgroup of $G$ for any $x \in X$ and $\{orb(x) : x \in X\}$ partitions the set $X$.*

**Theorem 4.3** *(Orbit-Stabilizer) Suppose $G$ acts on $X$, then for any $x \in X$*

$$|orb(x)| = [G : stab(x)]$$

**Theorem 4.4** *(Class equation)*

$$|G| = |Z(G)| + [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_n)]$$

*where $conj(a_1), conj(a_2), \ldots, conj(a_n)$ are the nontrivial conjugacy classes of $G$.*

**Corollary 4.5** *Every $p$-group has a nontrivial center, hence is not simple unless its isomorphic to $\mathbb{Z}_p$.*

**Corollary 4.6** *Groups of order $p^2$ are abelian.*

**Theorem 4.7** *(Sylow 1) If $G$ is a finite group and $p^n$ divides $|G|$, then there exists a subgroup $H \subseteq G$ with $|H| = p^n$.*

**Theorem 4.8** *(Sylow 2) If $G$ is a finite group, $H$ a p-subgroup of $G$, and $P$ a p-Sylow subgroup of $G$, then there exists $a \in G$ such that $H \subseteq aPa^{-1}$.*

**Corollary 4.9** *Let $G$ be a finite group such that $p$ divides $|G|$.*
*(a) Any p-subgroup of $G$ is contained in a p-Sylow subgroup of $G$.*
*(b) Any two p-Sylow subgroups of $G$ are conjugates.*
*(c) Any two p-Sylow subgroups of $G$ are isomorphic.*
*(d) A p-Sylow subgroup is of $G$ normal iff it is the only p-Sylow subgroup of $G$.*

**Theorem 4.10** *(Sylow 3) If $|G| = p^n m$ where $p$ does not divide $m$ and $n(p)$ is the number of p-Sylow subgroups of $G$, then:*
*(a) $n(p) = [G : N(P)]$ for any $P$ a p-Sylow subgroup of $G$,*
*(b) $n(p)$ divides $m$, and*
*(c) $n(p) = 1$ mod $p$*

# 5 Linear Transformations

In this section we consider only finite dimensional vector spaces $V$ or $W$ over an arbitrary field $\mathbb{F}$.

**Theorem 5.1** *Every linear transformation $L : \mathbb{F}^n \to \mathbb{F}^m$ is determined by an $m \times n$ matrix $A$:*

$$L(X) = AX$$

*for every $X \in \mathbb{F}^n$*

**Theorem 5.2** *Suppose $V$ and $W$ are vector space over a field $\mathbb{F}$.*
*If $\dim(V) = \dim(W)$, then $V$ is isomorphic to $W$.*

**Definition 5.3** *For $L : V \to W$ a linear transformation, define the null space (or kernel) of $L$, $\text{null}(L)$, and the range space of $L$, $\text{range}(L)$ as follows:*
*(a) $\text{null}(L) = \{v \in V : L(v) = z\}$*
*(b) $\text{range}(L) = \{w \in W :$ there exists $v \in V$ such that $L(v) = w\}$*

**Proposition 5.4** *$\text{null}(L)$ and $\text{range}(L)$ are subspaces of $V$ and $W$, respectively.*

**Theorem 5.5** *Suppose $L : V \to W$ is a linear transformation. Then*

$$\dim(V) = \dim(\text{null}(L)) + \dim(\text{range}(L)).$$

**Theorem 5.6** *Suppose $A, B \in \mathbb{F}^{n\times n}$, then $A$ is similar to $B$ iff there exists a basis $v_1, v_2, \ldots, v_n$ for $\mathbb{F}^{n\times 1}$ such that for every $j$*

$$\mathbf{A}(v_j) = \sum_{i=1}^{n} entry_{ij}(B) v_i.$$

*Furthermore, given such a basis if $P$ is the invertible matrix where $col_j(P) = v_j$ for each $j$, then $P$ witnesses their similarity, i.e., $A = PBP^{-1}$.*

# 6 Triangulizability

In this section we consider only square matrices over the field of complex numbers, $\mathbb{C}$. All vector spaces $V$, $W$, etc are assumed to be finite dimensional vector spaces over the complex numbers.

**Theorem 6.1** *Suppose for every linear transformation $L : V \to V$ that $V$ has a basis $v_1, v_2, \ldots, v_n$ such that*

$$L(v_k) \in \text{span}(\{v_1, \ldots, v_k\})$$

*for every $k$ with $1 < k \leq n$. Then every $n \times n$ matrix is similar to to an upper triangular matrix.*

**Theorem 6.2** *Suppose $V$ is a finite dimensional vector space over $\mathbb{C}$ and $L : V \to V$ is a linear transformation. Then there exists a nontrivial $v \in V$ and $\lambda \in \mathbb{C}$ such that $L(v) = \lambda v$.*

**Definition 6.3** *If $W_1$ and $W_2$ are subspaces of a vector space $V$ such that $W_1 \cap W_2 = \{\mathbf{0}\}$, then define*

$$W_1 \bigoplus W_2 = \{w_1 + w_2 : w_1 \in W_1, w_2 \in W_2\}.$$

*Whenever we write $W_1 \bigoplus W_2$ we will be assuming that $W_1 \cap W_2 = \{\mathbf{0}\}$.*

**Lemma 6.4** *For $V$ a vector space and $W_i$'s subspaces:*

*(a) $W_1 \bigoplus W_2$ is a subspace of $V$*

*(b) For any $u \in W_1 \bigoplus W_2$, $w_1, w_1' \in W_1$, and $w_2, w_2' \in W_2$, if $u = w_1 + w_2$ and $u = w_1' + w_2'$ then $w_1 = w_1'$ and $w_2 = w_2'$.*

*(c) If $B_1$ is a basis for $W_1$ and $B_2$ is a basis for $W_2$, then $B_1 \cup B_2$ is a basis for $W_1 \bigoplus W_2$.*

*(d) Given $W_1 \bigoplus W_2$ define $P : W_1 \bigoplus W_2 \to W_2$ by $P(w_1 + w_2) = w_2$ where $w_2 \in W_2$, and $w_1 \in W_1$, then $P$ is a linear transformation such that kernel$(P) = W_1$ and $P(v) = v$ for all $v \in W_2$. ($P$ is called a projection.)*

*(e) For any $W_1$ a subspace of a finite dimensional $V$ there exists $W_2$ a subspace of $V$ such $V = W_1 \bigoplus W_2$.*

**Lemma 6.5** *Suppose $L : V \to V$ is a linear transformation and $W \neq V$ a proper subspace of $V$. Then there exists $v \in V$ such that $v \notin W$ and $\lambda \in \mathbb{C}$ such that $L(v) - \lambda v \in W$.*

**Theorem 6.6** *Suppose $L : V \to V$ is a linear transformation. Then $V$ has a basis $v_1, v_2, \ldots, v_n$ such that for each $k = 1, \ldots, n$ $\quad L(v_k) \in span(\{v_1, v_2, \ldots, v_k\})$.*

**Corollary 6.7** *Every matrix $A \in \mathbb{C}^{n \times n}$ is similar to an upper triangular matrix.*

**Definition 6.8** *A sequence $u_1, u_2, \ldots, u_n$ in an inner product space is orthonormal iff for all $i, j$*

$$\langle u_i, u_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

**Proposition 6.9** *Orthonormal sequences are linearly independent.*

**Theorem 6.10** *(Gram-Schmidt Orthogonalization Process). If $v_1, v_2, \ldots, v_n$ and linear independent, then there exists $u_1, \ldots, u_n$ an orthonormal sequence such that for every $k = 1, \ldots, n$*

$$span(\{v_1, \ldots, v_k\}) = span(\{u_1, \ldots, u_k\}).$$

**Theorem 6.11** *Suppose $V$ is a finite dimensional inner product space and $L : V \to V$ is a linear transformation, then $V$ has an orthonormal basis $u_1, u_2, \ldots, u_n$ such that for each $k = 1, \ldots, n$*

$$L(u_k) \in span(\{u_1, u_2, \ldots, u_k\}).$$

**Corollary 6.12** *(Schur) For every matrix $A \in \mathbb{C}^{n \times n}$ there exists a unitary matrix $P$ (ie $P^{-1} = P^*$ the conjugate transpose) such that $P^{-1}AP$ is an upper triangular matrix.*

**Corollary 6.13** *If $A = A^*$ then $A$ is (unitarily) similar to a diagonal matrix all of whose entries are real. Hence all the eigenvalues of $A$ are real.*

# 7 Jordan Normal Form

In this section all vector spaces $V$, $W$, etc., are assumed to be finite dimensional vector spaces over an algebraically closed field $\mathbb{F}$, e.g., the complex numbers.

**Definition 7.1** *$\langle v_1, v_2, \ldots, v_n \rangle$ is an $L$-shifting sequence iff $v_1 \neq \mathbf{0}, L(v_1) = \mathbf{0}$ and $L(v_{k+1}) = v_k$ for each $k = 1, 2, \ldots, n-1$.*

**Definition 7.2** *For $W \subseteq V$ $L(W) = \{L(v) : v \in W\}$. It is the same as the range of $L$ when $W = V$.*

**Theorem 7.3** *An $L$-shifting sequence $\langle v_1, v_2, \ldots, v_n \rangle$, is linearly independent. Also if $W = span(\{v_1, v_2, \ldots, v_n\})$, then $L(W) \subseteq W$.*

**Theorem 7.4** *Suppose $L : V \to V$ is a linear transformation and let $W_1 = \{v \in V : \exists n \; L^n(v) = \mathbf{0}\}$. Then $L(W_1) \subseteq W_1$ and there exists $W_2$ with $L(W_2) \subseteq W_2$ such that $V = W_1 \bigoplus W_2$.*

**Definition 7.5** *Define a linear transformation $L : V \to V$ to be nilpotent iff for every $v \in V$ there exists $n$ such that $L^n(v) = \mathbf{0}$.*

**Theorem 7.6** *Suppose $L : V \to V$ is a nilpotent linear transformation. Then there exists $W_1, W_2$ such that $L(W_1) \subseteq W_1$, $L(W_2) \subseteq W_2$, $V = W_1 \bigoplus W_2$ and $W_1$ has an $L$-shifting sequence for a basis.*

**Definition 7.7** *The shift matrix $S$ is the square matrix such that $entry_{i,i+1}S = 1$ for each $i$ and all other entries of $S$ are $0$.*

**Definition 7.8** *Matrices of the form $J = \lambda I + S$ are called Jordan block matrices.*

**Theorem 7.9** *(Jordan normal form) Every square matrix $A$ is similar to a matrix in the block diagonal form:*

$$\begin{bmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & J_n \end{bmatrix}$$

*where each $J_i$ is a Jordan block matrix.*