1 Rank inequalities

Theorem 14.1. If $U$ and $V$ are subspaces of $W$, then $\dim(\text{Span}(U \cup V)) \leq \dim(U) + \dim(V)$.

Definition 14.2. If $U$ and $V$ are subspaces of $W$, then let $U + V = \{u + v \mid u \in U, v \in V\}$.

Exercise 14.3. If $U$ and $V$ are subspaces of $W$, then $\text{Span}(U \cup V) = U + V$.

Exercise 14.4 (Modular identity). $\dim(U + V) + \dim(U \cap V) = \dim(U) + \dim(V)$.

Corollary 14.5 (Submodular inequality). $S, T \subset V$ (subsets), then

$$\text{rk}(S) + \text{rk}(T) \geq \text{rk}(S \cap T) + \text{rk}(S \cup T).$$

This says that “rank is submodular.”

Theorem 14.6. If $A, B \in M_n(F)$, $\text{rk}(AB) \leq \min(\text{rk}(A), \text{rk}(B))$.

Corollary 14.7. $\text{rk}(AA^T) \leq \text{rk}(A)$ over any field.

Corollary 14.8. $\text{rk}(AA^*) \leq \text{rk}(A)$ over $\mathbb{C}$.

Exercise 14.9. $\text{rk}(AA^*) = \text{rk}(A)$ over $\mathbb{C}$, thus $\text{rk}(AA^T) = \text{rk}(A)$ over $\mathbb{R}$.

Exercise 14.10. Give examples of other fields of all characteristics such that $\text{rk}(AA^T) \neq \text{rk}(A)$.

2 Rings

Definition 14.11. A ring is a set $(R, +, \cdot)$ such that

- $(R, +)$ is an abelian group,
• (B) \((R \setminus \{0\}, \cdot)\) is a group,
• (C1) \((a + b)c = ac + bc\),
• (C2) \(a(b + c) = ab + ac\).

**Exercise 14.12.** \(0 + 0 = 0\).

**Definition 14.13.** \(a\) is a zero divisor if \(a \neq 0\) and \(\exists b \neq 0\) such that \(ab = 0\).

**Example 14.14.** \(\mathbb{Z}\) has no zero divisors.

**Example 14.15.** \(\mathbb{Z}/m\mathbb{Z}\) has zero divisors \(\iff m\) is composite.

**Example 14.16.** A field has no zero divisors.

**Exercise 14.17.** \(\mathbb{F}[x]\), the ring of polynomials over a field \(\mathbb{F}\), has no zero divisors.

**Remark 14.18.** \(M_n(\mathbb{F})\) is a non-commutative ring with zero divisors. Let

\[
A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.
\]

Then \(A^2 = 0\), so \(A\) is a zero divisor.

**Exercise 14.19.** \(A \in M_n(\mathbb{F})\) is a zero divisor \(\iff A\) is singular and non-zero.

**Exercise 14.20.** \(a \in \mathbb{Z}/m\mathbb{Z}\) is a zero divisor \(\iff a \neq 0\) and \(\gcd(a, m) > 1\).

**Definition 14.21.** An integral domain is a commutative ring with identity and no zero divisors.

**Example 14.22.** \(\mathbb{Z}\), any field \(\mathbb{F}\), and \(\mathbb{F}[x]\) are all integral domains.

### 3 Ideals

**Definition 14.23.** If \(\mathcal{I} \subseteq R\) is a subset of a ring, then \(\mathcal{I}\) is an ideal \((\mathcal{I} \triangleleft R)\) if

A) \(\mathcal{I}\) is an additive subgroup.

B) \((\forall a, b \in \mathcal{I})(\forall r \in R)(ar \in \mathcal{I})\).

**Example 14.24.** \(d\mathbb{Z} \triangleleft \mathbb{Z}\), where \(d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}\).

**Example 14.25.** If \(f \in \mathbb{F}[x]\), \(f\mathbb{F}[x] = \{fg \mid g \in \mathbb{F}[x]\} \triangleleft \mathbb{F}[x]\).

**Definition 14.26.** If \(R\) is a commutative ring with identity, \(u \in R\), then \((u) = \{ur \mid r \in R\}\) is called a principal ideal.
Exercise 14.27. Prove that this is an ideal.

Theorem 14.28. In $\mathbb{Z}$ and in $\mathbb{F}[x]$, every ideal is a principal ideal.

Example 14.29. In $\mathbb{Z}[x]$, not every ideal is a principal ideal. Indeed, consider the set of polynomials with even constant term. This is an ideal which is not principal.

Lemma 14.30 (Division theorem). $(\forall f, g)(\exists q, r)(g =fq +r$ and $\deg(r) < \deg(f)$.

Definition 14.31. Suppose $R$ is an integral domain, $f, g \in R$. $f \mid g$ if $\exists h \in R$ such that $fh = g$.

Definition 14.32. $d = \gcd(f, g)$ if

- $d \mid f$,
- $d \mid g$, and
- for every $e$ such that $e \mid f$ and $e \mid g$, we have that $e \mid d$.

Example 14.33. Everything is a divisor of 0, so $\gcd(0, 0) = 0$.

Definition 14.34. Divisors of 1 are called units. $g \mid 1$ means that $(\exists h)(gh = 1)$.

Definition 14.35. $R^\times$ is the set of units in $R$.

Exercise 14.36. $R^\times$ is a multiplicative group.

Example 14.37. $\mathbb{F}[x]^\times = \mathbb{F}^\times$.

Example 14.38. $\mathbb{Z}[x]^\times = \{\pm 1\}$.

Definition 14.39. The Gaussian integers are the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Exercise 14.40. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Exercise 14.41. Every ideal in $\mathbb{Z}[i]$ is a principal ideal. Hint: invent a division theorem for Gaussian integers.

Definition 14.42. $R$ is a principal ideal domain (PID) if $R$ is an integral domain and all ideals of $R$ are principal.

Example 14.43. $\mathbb{Z}$, $\mathbb{F}[x]$, and $\mathbb{Z}[x]$ are all principal ideal domains.

Exercise 14.44. In $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, the g.c.d. does not exist (that is not every pair of elements has a g.c.d.).

Theorem 14.45. If $R$ is a PID, then $gcd$ always exists and is a linear combination:

$(\forall f, g \in R)(\exists d = \gcd(f, g) \text{ and } \exists r, s \in R \text{ such that } d = rf + sg)$.

Definition 14.46. $f \in \mathbb{F}[x]$ is irreducible if $f \neq 0$, $f$ is not a unit, and whenever $f = gh$, either $g$ or $h$ is a unit.
4 Minimal polynomial

Henceforth, “irreducible polynomial” will mean irreducible over $\mathbb{Q}$, when no other field is indicated.

**Definition 14.47.** Assume that $\alpha \in \mathbb{C}$. Then $\mathcal{I}_\alpha = \{ f \in \mathbb{Q}[x] \mid f(\alpha) = 0 \} \triangleleft \mathbb{Q}[x]$. This is principal. Thus $\mathcal{I}_\alpha = (m_\alpha)$, and $m_\alpha$ is the minimal polynomial of $\alpha$.

**Corollary 14.48.** If $f \in \mathbb{Q}[x]$, $f \alpha = 0 \iff m_\alpha \mid f_\alpha$.

**Exercise 14.49.** $m_\alpha$ is irreducible.

**Exercise 14.50.** If $f \in \mathbb{Q}[x]$, $f \alpha = 0$, and $f$ is irreducible, then $f = cm_\alpha$ for some unit $c$.

**Exercise 14.51.** $x^3 - 2$ is irreducible.

**Corollary 14.52.** $m_{\sqrt[3]{2}}(x) = x^3 - 2$.

**Definition 14.53.** $\alpha$ is algebraic if $m_\alpha \neq 0$. i.e. $\exists f \in \mathbb{Q}[x] \setminus \{0\}$ such that $f \alpha = 0$.

**Definition 14.54.** If $\alpha$ is not algebraic, then it is called transcendental.

**Definition 14.55.** If $\alpha$ is algebraic, then $\deg(\alpha) = \deg(m_\alpha)$.

**Example 14.56.** $\deg(\sqrt[3]{2}) = 3$.

**Example 14.57.** $q \in \mathbb{Q} \Rightarrow \deg(q) = 1$.

**Exercise 14.58.** $x^n - 2$ is irreducible.

**Definition 14.59.** $\mathbb{Q}[\alpha] = \{ f(\alpha) \mid f \in \mathbb{Q}[\alpha] \}$.

**Theorem 14.60.** If $\alpha$ is algebraic, $\deg(\alpha) = k \geq 1$, then

$$\mathbb{Q}[\alpha] = \{ a_0 + a_1 \alpha + \cdots + a_k \alpha^{k-1} \mid a_j \in \mathbb{Q} \}.$$

**Exercise 14.61.** $\dim_{\mathbb{Q}}(\mathbb{Q}[\alpha]) = \deg(\alpha)$.

**Theorem 14.62.** If $\alpha$ is algebraic, then $\mathbb{Q}[\alpha]$ is a field.

**Theorem 14.63.** If $\mathbb{F}$ is any field and $\alpha$ is algebraic over $\mathbb{F}$, then $\mathbb{F}[\alpha]$ is a field.

**Theorem 14.64.** The set of algebraic numbers is a field.

In fact, we will prove that:

$$\deg(\alpha \pm \beta) \leq \deg(\alpha)\deg(\beta)$$

$$\deg(\alpha \beta) \leq \deg(\alpha)\deg(\beta)$$

$$\deg(\alpha/\beta) \leq \deg(\alpha)\deg(\beta)$$
Exercise 14.65. Find \( m \sqrt[3]{3} + \sqrt[7]{7} \).

Theorem 14.66. If \( K \subseteq L \subseteq M \) are fields, then \( \dim_K(M) = \dim_L(M) \dim_K(L) \).

Exercise 14.67. If \( K \subseteq L \subseteq M \) are fields, \( \alpha_1, \ldots, \alpha_r \) is a basis of \( L \) over \( K \), and \( \beta_1, \ldots, \beta_s \) is a basis of \( M \) over \( L \), then \( \{ \alpha_j \beta_k \} \) is a basis of \( L \) over \( K \).

Exercise 14.68. If \( K \subseteq L \) are fields, and \( \alpha \) is algebraic over \( K \), then \( \deg_L(\alpha) \leq \deg_K(\alpha) \).

Theorem 14.69. If \( K \subseteq L \) are fields, and \( \dim_K(L) = k < \infty \) ("\( L \) is an extension of \( K \) of degree \( k \)), then every \( \alpha \in L \) is algebraic over \( K \) and \( \deg_K(\alpha) \mid k \).

Given an interval of unit linegth, can we construct with straightedge and compass an interval of length \( \sqrt[3]{2} \)? Galois showed that this is impossible. One observes that it is possible to construct the field \( \mathbb{Q} \), and beyond \( \mathbb{Q} \), any number constructed gives at most a degree two extension. Since to construct \( \sqrt[3]{2} \), one would need to form an extension of degree a multiple of three, this number is not constructible.

Definition 14.70. 
\[
J(k, \lambda) = \begin{pmatrix}
\lambda & 1 & 0 & \cdots & 0 \\
0 & \lambda & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & 0 \\
\vdots & \ddots & \ddots & 1 & 0 \\
0 & \cdots & 0 & \cdots & \lambda
\end{pmatrix}
\]
is the \( k \times k \) Jordan block with eigenvalue \( \lambda \).

Definition 14.71. A block diagonal matrix is a matrix 
\[
\text{diag}(A_1, \ldots, A_k) = \begin{pmatrix} A_1 & & \\
& A_2 & \\
& & \ddots \\
& & & A_k \end{pmatrix}
\]
such that the diagonal entries, \( A_j \) are all square matrices of varied sizes, \( n_j \times n_j \). It has dimension \( n \times n \), where \( n = \sum n_j \).

Exercise 14.72. The characteristic polynomial has the form: 
\[
f_{\text{diag}(A_1, \ldots, A_k)}(x) = \prod_{j=1}^{k} f_{A_j}(x).
\]

Theorem 14.73. If \( f \in \mathbb{F}[x] \), then \( f(\text{diag}(A_1, \ldots, A_k)) = \text{diag}(fA_1, \ldots, fA_k) \).

Corollary 14.74. \( m_{\text{diag}(A_1, \ldots, A_k)} = \text{L.c.m.}(f_{A_1}, \ldots, f_{A_k}) \).
Theorem 14.75. $\mathcal{I}_A = \{ f \in \mathbb{F}[x] \mid fA = 0 \} \triangleleft \mathbb{F}[x]$. Thus $\mathcal{I}_A = (m_A)$.

Definition 14.76. A Jordan normal form matrix is a block diagonal matrix with each block a Jordan block.

Theorem 14.77. $f_{\lambda,k}(x) = (x - \lambda)^k$.

Exercise 14.78. $m_{\lambda,k}(x) = (x - \lambda)^k$.

Corollary 14.79. A Jordan block is diagonalizable if and only if $k = 1$.

Definition 14.80. $A$ is similar to $B$ ($A \sim B$) if there exists $S$ such that $S^{-1}AS = B$.

Exercise 14.81. Two Jordan normal form matrices are similar if and only if they consist of the same blocks (possibly in a different order).

Theorem 14.82. If $\mathbb{F}$ is algebraically closed, then $\forall A \exists B$ such that $B$ is Jordan normal form and $B \sim A$.

Observe that if $f(A) = 0$, and $B \sim A$, then

$$f(B) = f(S^{-1}AS) = S^{-1}f(A)S = 0.$$ 

Exercise 14.83. If $f \in \mathbb{F}[x] \setminus \{0\}$ and $\mathbb{F}$ is algebraically closed, then for all $n$, the number of pairwise dissimilar solutions, $A \in M_n(\mathbb{F})$, to $fA = 0$ is finite (bounded by a function in $n$ and $\deg(f)$).

Theorem 14.84. If $A, B \in M_n(K)$, $L \supset K$ is a field extension, and $A \sim B$ over $L$, then $A \sim B$ over $K$.

Corollary 14.85. We may drop the condition of algebraic closure in Exercise ??.