Chapter 1

Vector Spaces

1.1 Groups and Abelian Groups

Definition 1.1. A binary operation on a set G is a mapping from $G \times G$ to G.

Definition 1.2. A binary operation $\star$ on a set G is called *associative* if for all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$ holds.

Definition 1.3. Let G be a set and $\star$ be a binary operation on G. An *identity* of G with respect to $\star$ is an element $e \in G$ such that $a \star e = a$ and $e \star a = a$ for all $a \in G$.

Theorem 1.4. The identity of G with respect to $\star$ is unique if it exists.

Proof. If e and e' are identity of G with respect to $\star$, then $e = e \star e' = e'$. □

Notation. The identity of G is denoted by 1_G. However, if the binary operation is written additively, the identity is denoted by 0_G instead.

Definition 1.5. Let $\star$ be a binary operation on G with identity e. Let a be an element of G. An element $b \in G$ is called an *inverse* of a if $a \star b = e$ and $b \star a = e$.

Theorem 1.6. For all $a \in G$, the inverse of $a \in G$ is unique if it exists.

Proof. If both b and b' are inverses of a, then

$$b = b \star 1_G = b \star (a \star b') = (b \star a) \star b' = 1_G \star b' = b'.$$ □

Notation. The inverse of a in G is denoted by a^{-1}. However, if the binary operation is written additively, the inverse of a is denoted by $-a$ instead.

Definition 1.7. A set G and a binary operation $\star$ on G form a *group* $(G, \star)$ if the following conditions hold.

(a) The operation $\star$ is associative.

(b) 1_G exists.

(c) For all $a \in G$, a^{-1} exists.

Example. Let S denote the set of permutations of $\{1, 2, 3\}$ and $\circ$ denote the composition of permutations. Then $(S, \circ)$ is a group.

Definition 1.8. A binary operation $\star$ on a set G is called *commutative* if for all $a, b, \in G$, $a \star b = b \star a$ holds.

Definition 1.9. A group $(G, \star)$ is called an *Abelian group* if $\star$ is commutative.

Example. $(\mathbb{Z}, +)$ and $(\mathbb{Q} \setminus \{0\}, \cdot)$ are Abelian groups.

Theorem 1.10. Let $(G, \star)$ be a group. Then for all $a \in G$, $(a^{-1})^{-1} = a$.

Proof. Since $a \star a^{-1} = 1_G$, a is the inverse of a^{-1} in G. Thus, $(a^{-1})^{-1} = a$. $\square$

Theorem 1.11 (Cancellation Law)**.** Let $(G, \star)$ be a group. Then the following statements are true.

(a) For all $a, b, c \in G$, if $c \star a = c \star b$, then $a = b$.

(b) For all $a, b, c \in G$, if $a \star c = b \star c$, then $a = b$.

Proof.

(a) We have

$$a = 1_G \star a = (c^{-1} \star c) \star a = c^{-1} \star (c \star a)$$

and

$$b = 1_G \star b = (c^{-1} \star c) \star b = c^{-1} \star (c \star b).$$

Because $c \star a = c \star b$, we have $a = b$.

(b) The proof is similar to (a). $\square$

1.2 Fields

Definition 1.12. Let F be a set. Let $+$ and $\cdot$ be binary operations on F.

(a) The operation $\cdot$ is called *left-distributive* over $+$ if $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

(b) The operation $\cdot$ is called *right-distributive* over $+$ if $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in F$.

(c) The operation $\cdot$ is called *distributive* over $+$ if it is both left-distributive and right-distributive.

Definition 1.13. A set F and two binary operations $+$ and $\cdot$ on F form a *field* $(F, +, \cdot)$ if the following conditions hold.

- $(F, +)$ is an Abelian group.
- $(F \setminus \{0_F\}, \cdot)$ is an Abelian group.
- The operation $\cdot$ is distributive over the operation $+$.

Example. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are fields.

Example. $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a field, where

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Theorem 1.14. Let $(F, +, \cdot)$ be a field. Then the following statements are true.

(a) For all $a \in F$, $a \cdot 0_F = 0_F = 0_F \cdot a$.

(b) For all $a, b \in F$, $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

(c) For all $a, b \in F$, $(-a) \cdot (-b) = a \cdot b$.

Proof.

(a) We have
$$a \cdot 0_F + a \cdot 0_F = a \cdot (0_F + 0_F) = a \cdot 0_F = a \cdot 0_F + 0_F.$$
Thus, $a \cdot 0_F = 0_F$ by cancelltaion law (Theorem 1.11). The proof of $0_F \cdot a = 0_F$ is similar.

(b) By (a), we have
$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0_F \cdot b = 0_F.$$
Thus, $(-a) \cdot b = -(a \cdot b)$. The proof of $a \cdot (-b) = -(a \cdot b)$ is similar.

(c) We have
$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$$
by applying (b) twice. $\square$

Remark. Let $G = F \setminus \{0_F\}$ and 1_G be the multiplicative identity of G. By Theorem 1.14 (a), we have $1_G \cdot 0_F = 0_F = 0_F \cdot 1_G$. Therefore, 1_G is also the multiplicative identity of F, and thus we denote it by 1_F.

Remark. Subtraction and division are defined in terms of addition and multiplication by using additive and multiplicative inverses.

1.3 Vector Spaces

Definition 1.15. Let F be a field. A set V and two operations $+ : V \times V \to V$, $\cdot : F \times V \to V$ form a *vector space* over F if the following conditions hold.

(a) $(V, +)$ is an Abelian group.

(b) For all $x \in V$, $1_F \cdot x = x$.

(c) For all $a, b \in F$ and for all $x \in V$, $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.

(d) For all $a, b \in F$ and for all $x \in V$, $(a + b) \cdot x = a \cdot x + b \cdot x$.

(e) For all $a \in F$ and for all $x, y \in V$, $a \cdot (x + y) = a \cdot x + a \cdot y$.

Example. $(F^n, +, \cdot)$ is a vector space over F.

Example. Let $\mathcal{P}(F)$ denote the set of polynomials with coefficients in F. Then $(\mathcal{P}(F), +, \cdot)$ is a vector space over F.

Example. Let $\mathcal{F}(S, F)$ denote the set of functions from S to F. Then $(\mathcal{F}(S, F), +, \cdot)$ is a vector space over F.

Theorem 1.16. Let $(V, +, \cdot)$ be a vector space over F. Then the following statements are true.

(a) For all $x \in V$, $0_F \cdot x = 0_V$.

(b) For all $a \in F$, $a \cdot 0_V = 0_V$.

(c) For all $a \in F$ and $x \in V$, $(-a) \cdot x = -(a \cdot x) = a \cdot (-x)$.

Proof.

(a) We have
$$0_F \cdot x + 0_F \cdot x = (0_F + 0_F) \cdot x = 0_F \cdot x = 0_F \cdot x + 0_V.$$
Thus, $0_F \cdot x = 0_V$ by cancelltaion law (Theorem 1.11).

(b) It is similar to the proof of (a).

(c) By (a), we have
$$a \cdot x + (-a) \cdot x = (a + (-a)) \cdot x = 0_F \cdot x = 0_V.$$
Thus, $(-a) \cdot x = -(a \cdot x)$. By (b), we have
$$a \cdot x + a \cdot (-x) = a \cdot (x + (-x)) = a \cdot 0_V = 0_V.$$
Thus, $a \cdot (-x) = -(a \cdot x)$. $\square$

1.4 Subspaces

Definition 1.17. Let $(V, +_V, \cdot_V)$ be a vector space over a field F. Let W be a subset of V. If $+_W : W \times W \to W$ and $\cdot_W : F \times W \to W$ satisfy

$$x +_W y = x +_V y \quad \text{and} \quad a \cdot_W x = a \cdot_V x$$

for all $a \in F$ and $x, y \in W$, then we say that $+_W$ and $\cdot_W$ *inherit* $+_V$ and $\cdot_V$, respectively.

Definition 1.18. Let $(V, +_V, \cdot_V)$ be a vector space over F. A subset W of V is called a *subspace* of V if $(W, +_W, \cdot_W)$ is a vector space over F, where $+_W$ and $\cdot_W$ inherit $+_V$ and $\cdot_V$, respectively.

Theorem 1.19. Let $(V, +_V, \cdot_V)$ be a vector space over F. Let W be a subset of V. Then W is a subspace of V if the following conditions hold.

(a) For all $x, y \in W$, $x +_V y \in W$.

(b) For all $a \in F$ and $x \in W$, $a \cdot_V x \in W$.

(c) $0_V \in W$.

Proof. We can define operations $+_W : W \times W \to W$ and $\cdot_W : F \times W \to W$ such that

$$x +_W y = x +_V y \quad \text{and} \quad a \cdot_W x = a \cdot_V x$$

for all $a \in F$ and $x, y \in W$ due to (a) and (b). Then according to Definition 1.17, $+_W$ and $\cdot_W$ inherit $+_V$ and $\cdot_V$, respectively.

Now we prove that $(W, +_W, \cdot_W)$ is a vector space over F. Since a vector in W is also in V, properties (b), (c), (d), and (e) in Definition 1.18 hold trivially. Thus, one only needs to check property (a) in Definition 1.18, i.e., $(W, +_W)$ is an Abelian group.

Since $+_W$ inherits $+_V$, $+_V$ is associative implies that $+_W$ is associative. Furthermore, since

$$0_V \in W \quad \text{and} \quad -x = -(1_F \cdot x) = (-1_F) \cdot x \in W$$

hold for all $x \in W$, we have

$$0_V +_W x = x = x +_W 0_V \quad \text{and} \quad x +_W (-x) = 0_V = (-x) +_W x$$

hold for all $x \in W$. Thus, $0_V \in W$ is an additive identity of W, and each vector in W also has an additive inverse in W, which complete the proof. $\square$

Example. Let $\mathcal{P}_n(F)$ denote the set of polynomials in $\mathcal{P}(F)$ with degree less than or equal to n, where $n \geq -1$ is an integer. Then it follows from Theorem 1.19 that $\mathcal{P}_n(F)$ is a subspace of $\mathcal{P}(F)$.

Theorem 1.20. Let $(V, +_V, \cdot_V)$ be a vector space over F. Let I be an index set such that W_i is a subspace of V for all $i \in I$. Then the intersection

$$W = \bigcap_{i \in I} W_i$$

is a subspace of V.

Proof. For all $a \in F$ and for all $x, y \in W$, since

$$x +_V y \in W_i \quad \text{and} \quad a \cdot_V x \in W_i \quad \text{and} \quad 0_V \in W_i$$

hold for all indices $i \in I$, we have

$$x +_V y \in W \quad \text{and} \quad a \cdot_V x \in W \quad \text{and} \quad 0_V \in W.$$

Thus, W is a subspace of V. $\square$

Definition 1.21. Let $(V, +_V, \cdot_V)$ be a vector space over F. Let S_1 and S_2 be subsets of V. Then the *sum* of S_1 and S_2, denoted $S_1 + S_2$, is the set $\{x + y : x \in S_1 \text{ and } y \in S_2\}$.

Theorem 1.22. Let $(V, +_V, \cdot_V)$ be a vector space over F. If W_1 and W_2 be subspaces of V, then the following statements are true.

(a) $W_1 + W_2$ is a subspace of V.

(b) If W is a subspace of V with $W_1 \cup W_2 \subseteq W$, then $W_1 + W_2 \subseteq W$.

Proof.

(a) Suppose that $a \in F$ and $x, y \in W_1 + W_2$. Then there exists $x_1, y_1 \in W_1$ and $x_2, y_2 \in W_2$ such that

$$x = x_1 +_V x_2 \quad \text{and} \quad y = y_1 +_V y_2.$$

Thus,

$$a \cdot_V x = a \cdot_V (x_1 + x_2) = a \cdot_V x_1 + a \cdot_V x_2 \in W_1 + W_2$$

and

$$x +_V y = (x_1 +_V x_2) + (y_1 +_V y_2) = (x_1 +_V y_1) + (x_2 +_V y_2) \in W_1 + W_2.$$

We also have $0_V = 0_V +_V 0_V \in W_1 + W_2$. Hence, $W_1 + W_2$ is a subspace of V.

(b) If $x \in W_1 + W_2$, then there exists $x_1 \in W_1$ and $x_2 \in W_2$ such that $x = x_1 + x_2$. Since $W_1 \subseteq W$ and $W_2 \subseteq W$, we have $x_1 \in W$ and $x_2 \in W$, which implies $x \in W$. $\square$

1.5 Spanning Sets

Definition 1.23. Let $(G,+)$ be an Abelian group. Then we define

$$\sum_{i=m}^{n} a_i = \begin{cases} \displaystyle\sum_{i=m}^{n-1} a_i + a_n & \text{if } m \leq n \\ 0_G & \text{if } m > n, \end{cases}$$

where $a_i \in G$ for each integer i with $m \leq i \leq n$.

Definition 1.24. Let $(V,+,\cdot)$ be a vector space over F. Let S be a subset of V. Then a vector $x \in V$ is called a *linear combination* of S if there exists some nonnegative integer n such that

$$x = \sum_{i=1}^{n} a_i x_i,$$

where $a_i \in F$ and $x_i \in S$ for each integer i with $1 \leq i \leq n$.

Remark. Since n can be zero, 0_V is a linear combination for all $S \subseteq V$.

Remark. Although S can be infinite, the number of terms in the summation must be finite. For example, although we have

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \cdots,$$

e is not a linear combination of $\mathbb{Q}$ in the vector space $\mathbb{R}$ over $\mathbb{Q}$ since the number of terms is the summation is infinite.

Definition 1.25. Let $(V,+,\cdot)$ is a vector space over F. The *span* of S, denoted $\operatorname{span}(S)$, is the set that consists of all linear combinations of S.

Theorem 1.26. Let $(V,+,\cdot)$ be a vector space over F. Let $S \subseteq V$. Then the following statements are true.

(a) $\operatorname{span}(S)$ is a subspace of V.

(b) If W is a subspace of V such that $S \subseteq W$, then $\operatorname{span}(S) \subseteq W$.

Proof.

(a) If $c \in F$ and $x, y \in \operatorname{span}(S)$, then there exist nonnegative integers m, n, scalars $a_1, \ldots, a_m, b_1, \ldots, b_n \in F$ and vectors $x_1, \ldots, x_m, y_1, \ldots, y_n \in S$ such that

$$x = \sum_{i=1}^{m} a_i x_i \quad \text{and} \quad y = \sum_{j=1}^{n} b_j y_j.$$

Thus, we have

$$\begin{aligned} cx &= c(a_1x_1 + \cdots + a_mx_m) \\ &= c(a_1x_1) + \cdots + c(a_mx_m) \\ &= (ca_1)x_1 + \cdots + (ca_m)x_m \in \operatorname{span}(S) \end{aligned}$$

and

$$x + y = a_1x_1 + \cdots a_mx_m + b_1y_1 + \cdots + b_ny_n \in \operatorname{span}(S).$$

Also, $0_V \in \operatorname{span}(S)$. Hence, $\operatorname{span}(S)$ is a subspace of V.

(b) If $x \in \operatorname{span}(S)$, then there exists an nonnegative integer n, scalars $a_1, \ldots, a_n \in F$ and vectors $x_1, \ldots, x_n \in S$ such that

$$x = \sum_{i=1}^{m} a_i x_i.$$

Thus, since $x_1, \ldots, x_n \in W$, we have $x = a_1 x_1 + \cdots + a_n x_n \in W$. $\square$

Definition 1.27. A subset S of a vector space $(V, +, \cdot)$ *spans* V if $\operatorname{span}(S) = V$. In this case, we also say that S is a *spanning set* of V.

Example. $\{(1,1,0), (0,1,1), (1,0,1)\}$ is a spanning set of $\mathbb{R}^3$ since for all $x, y, z \in \mathbb{R}$,

$$(x, y, z) = \frac{x + y - z}{2} \cdot (1,1,0) + \frac{-x + y + z}{2} \cdot (0,1,1) + \frac{x - y + z}{2} \cdot (1,0,1).$$

1.6 Linearly Independent Sets

Definition 1.28. Let $(V, +, \cdot)$ be a vector space over F.

(a) A subset S of V is called *linearly dependent* if there is an element $x \in S$ with $x \in \operatorname{span}(S \setminus \{x\})$.

(b) A subset S of V is called *linearly independent* if it is not linear dependent.

Theorem 1.29. Let $(V, +, \cdot)$ be a vector space over F. Then a subset S of V is linearly dependent if and only if there exist a positive integer n, scalars $a_1, \ldots, a_n \in F$, and distinct vectors $x_1, \ldots, x_n \in S$ such that

$$\sum_{i=1}^{n} a_i x_i = 0_V,$$

where there exists an integer $i \in \{1, \ldots, n\}$ such that $a_i \neq 0_F$.

Proof. $(\Rightarrow)$ Since S is linearly dependent, there exists $x \in S$ with $x \in \operatorname{span}(S \setminus \{x\})$. Thus, there exist m scalars $a_1, \ldots, a_m \in F$ and m distinct vectors $x_1, \ldots, x_m \in S \setminus \{x\}$ such that

$$x = a_1 x_1 + \cdots + a_m x_m,$$

which implies

$$a_1 x_1 + \cdots + a_m x_m + (-1_F)x = 0_V.$$

$(\Leftarrow)$ Suppose that there are n scalars $a_1, \ldots, a_n \in F$ and n distinct vectors $x_1, \ldots, x_n \in S$, where $a_1 \neq 0_F$, such that

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0_V.$$

Then we have

$$\begin{aligned} x_1 &= a_1^{-1}(a_1 x_1) \\ &= a_1^{-1}(-(a_2 x_2 + \cdots + a_n x_n)) \\ &= (-a_1^{-1} a_2) x_2 + \cdots + (-a_1^{-1} a_n) x_n \\ &\in \operatorname{span}(S \setminus \{x_1\}). \end{aligned}$$

Thus, S is linearly dependent. $\square$

Example. Let $S = \{1, 1+2x, 1+2x+3x^2, 1+2x+3x^2+4x^3\}$ be a subset of $\mathcal{P}_3(\mathbb{R})$. Then S is linearly independent since the only solution to the following system of linear equations

$$\begin{aligned} &a_1 &&= 0 \\ &a_1 + 2a_2 &&= 0 \\ &a_1 + 2a_2 + 3a_3 &&= 0 \\ &a_1 + 2a_2 + 3a_3 + 4a_4 &&= 0 \end{aligned}$$

is $a_1 = a_2 = a_3 = a_4 = 0$.

Theorem 1.30. Let $(V, +, \cdot)$ be a vector space, and let $R \subseteq S \subseteq V$. If R is linearly dependent, then S is linearly dependent.

Proof. If R is linearly dependent, then there exists $x \in R$ such that $x \in \text{span}(R \setminus \{x\})$. By $R \subseteq S$, we have $R \setminus \{x\} \subseteq S \setminus \{x\}$. Since $x \in S$ and $x \in \text{span}(S \setminus \{x\})$, S is linearly dependent. $\square$

Corollary. Let $(V, +, \cdot)$ be a vector space, and let $R \subseteq S \subseteq V$. If S is linearly independent, then R is linearly independent.

Proof. Suppose that S is linearly independent. If R is linearly dependent, then so is S by Theorem 1.30, contradiction. Thus, R is linearly independent. $\square$

Theorem 1.31. Let $(V, +, \cdot)$ be a vector space. For each finite set $S \subseteq V$, there exists a linearly independent set $R \subseteq S$ such that $\text{span}(R) = \text{span}(S)$.

Proof. The proof is by induction on $n = |S|$. The induction begins with $n = 0$, i.e., $S = \varnothing$. Since $\varnothing$ is linearly independent, we can choose $R = \varnothing$, and thus the theorem holds.

Now suppose that the theorem is true for some integer $n \geq 0$, and we prove that the theorem holds for $n + 1$. If S is linearly independent, then we can choose $R = S$. Otherwise, there exists $x \in S$ with $\text{span}(S \setminus \{x\}) = \text{span}(S)$ because S is linearly dependent. Let $S' = S \setminus \{x\}$. Then there exists a linearly independent set $R \subseteq S'$ such that $\text{span}(R) = \text{span}(S')$ by induction hypothesis, implying $R \subseteq S$ and $\text{span}(R) = \text{span}(S)$. $\square$

1.7 Bases and Dimension

Definition 1.32. Let $(V, +, \cdot)$ be a vector space. A subset S of V is a *basis* of V if S is not only a spanning set but also a linearly independent set of V.

Example. Since $\operatorname{span}(\varnothing) = \{0_V\}$ and $\varnothing$ is linearly independent, $\varnothing$ is a basis of $\{0_V\}$.

Example. Let $S = \{x_1, \ldots, x_n\}$ be a subset of F^n with $(x_i)_j = [\![i = j]\!]$ for all $i, j \in \{1, \ldots, n\}$. Then S is called the *standard basis* of F^n.

Example. The set $S = \{1_F, x, x^2, \ldots, x^n\}$ is the called the *standard basis* of $\mathcal{P}_n(F)$.

Theorem 1.33. Let $(V, +, \cdot)$ be a vector space over F. If there exists a finite set S that spans V, then V has a finite basis.

Theorem 1.34 (Replacement Theorem)**.** Let $(V, +, \cdot)$ be a vector space over F. Let S be a finite set of n vectors that spans V, and let $Q \subseteq V$ be a finite linearly independent set of m vectors. Then there exists $R \subseteq S \setminus Q$ such that both $|Q \cup R| = |S|$ and $\operatorname{span}(Q \cup R) = V$ hold.

Proof. The proof is based on induction on m. The induction begins with $m = 0$, i.e., $Q = \varnothing$. Choosing $R = S$, we have $Q \cup R = S$, and thus both $|Q \cup R| = S$ and $\operatorname{span}(Q \cup R) = V$ hold.

Now suppose that the theorem is true for some integer $m \geq 0$, and we prove that the theorem holds for $m+1$. Let $Q = \{x_1, \ldots, x_{m+1}\}$ and let $Q' = Q \setminus \{x_{m+1}\}$. By induction hypothesis, there exists $R' = \{y_1, \ldots, y_{n-m}\} \subseteq S \setminus Q'$ such that $\operatorname{span}(Q' \cup R') = V$. Since $Q' \cup R'$ spans V, there exists $a_1, \ldots, a_m, b_1, \ldots, b_{n-m} \in F$ such that

$$x_{m+1} = \sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{n-m} b_i y_i.$$

There must exist some $j \in \{1, \ldots, n-m\}$ such that $b_j \neq 0_F$. Otherwise, we have $x_m \in \operatorname{span}(Q')$, implying that Q is not linearly independent, contradiction. Without loss of generality let $b_{n-m} \neq 0_F$. Also, let $R = \{y_1, \ldots, y_{n-m-1}\}$. Then $|Q \cup R| = |S|$.

Note that $(Q' \cup R') \setminus (Q \cup R) = \{y_{n-m}\}$. Since

$$y_{n-m} = (-b_j)^{-1} \left(-x_{m+1} + \sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{n-m-1} b_i y_i \right) \in \operatorname{span}(Q \cup R),$$

we have $Q' \cup R' \subseteq \operatorname{span}(Q \cup R)$. Thus, by Theorem 1.26 we have

$$V = \operatorname{span}(Q' \cup R') \subseteq \operatorname{span}(Q \cup R) \subseteq V,$$

implying $\operatorname{span}(Q \cup R) = V$. $\square$

Corollary. Let $(V, +, \cdot)$ be a vector space over F. Let S be a finite spanning set of V and let $Q \subseteq V$ be a linearly independent set. Then $|Q| \leq |S|$.

Proof. Suppose that $|Q| > |S|$. Then there exists a subset $Q' \subseteq Q$ with $|Q'| = |S| + 1$. Q' is linearly independent because Q is linearly independent. Then, by Theorem 1.34 there exists $R' \subseteq S \setminus Q'$ such that $|Q' \cup R'| = |S|$. However, $|Q' \cup R'| \geq |Q'| > |S|$, contradiction. Thus, $|Q| \leq |S|$. $\square$