Review.

Example. Let V be an n-dimensional vector space.

a. If $v_1, \ldots, v_n$ is independent, then it is a basis.

b. If $v_1, \ldots, v_n$ spans, then it is a basis.

Proof. a. Suppose $v_1, \ldots, v_n$ is independent. An independent set can be enlarged to a basis, so let $v_1, \ldots, v_n \subset \mathcal{B}$, where $\mathcal{B}$ is a basis.

Since $\dim V = n$, and since any two bases for V have the same cardinality, $|\mathcal{B}| = n$. But $v_1, \ldots, v_n$ has n elements, so $v_1, \ldots, v_n = \mathcal{B}$. Therefore, $v_1, \ldots, v_n$ is a basis.

b. Suppose $v_1, \ldots, v_n$ spans. A spanning set contains a subset which is a basis, so let $\mathcal{B} \subset v_1, \ldots, v_n$, where $\mathcal{B}$ is a basis.

Since $\dim V = n$, and since any two bases for V have the same cardinality, $|\mathcal{B}| = n$. But $v_1, \ldots, v_n$ has n elements, so $v_1, \ldots, v_n = \mathcal{B}$. Therefore, $v_1, \ldots, v_n$ is a basis. $\square$

Here's an example. Consider the set of vectors

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ -2 \end{bmatrix}, \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ -1 \end{bmatrix} \right\}.$$

This is a set of 3 vectors in the 3-dimensional space $\mathbb{R}^3$.

To show that this set is a basis, it suffices to show that the set is independent. Form the matrix whose rows are the vectors and row reduce:

$$\begin{bmatrix} 1 & 0 & -2 \\ -1 & 3 & 1 \\ 2 & 4 & -1 \end{bmatrix} \quad \to \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The row reduced matrix has rank 3 (3 leading coefficients, or equivalently, 3 nonzero rows). Therefore, the original set was independent, hence a basis. $\square$

Example. Show that the preceding result is false if the vector space is infinite dimensional (and "n" is replaced by an appropriate cardinal number).

Let $V = \mathbb{R}[x]$, regarded as a vector space over $\mathbb{R}$. V is infinite dimensional, and

$$\mathcal{B} = \{1, x, x^2, x^3, \ldots\}$$

is a basis for V.

The set

$$x^2, x^4, x^6, \ldots$$

is independent, and has the same cardinality as $\mathcal{B}$. However, it is not a basis, since it does not span — no linear combination of even powers of x will yield an odd power of x (or a nonzero constant, for that matter). $\square$

Example. The definition of a basis is a maximal linearly independent set. It is easy to show that a basis spans. The converse is also true.

Lemma. A linearly independent spanning set is a basis.

Proof. Let $\mathcal{B}$ be a linearly independent spanning set. I must show that it is a maximal independent set.

Let $\mathcal{B} \subset \mathcal{C}$, where $\mathcal{C}$ is independent. I must show that the two sets are equal. Let $w \in \mathcal{C}$. Since $\mathcal{B}$ spans,

$$w = a_1 v_1 + \cdots a_n v_n, \qquad a_i \in F,$$

and $v_1, \ldots, v_n$ are distinct elements of $\mathcal{B}$.

Therefore,

$$a_1 v_1 + \cdots a_n v_n - w = 0,$$

which is a nontrivial linear relation among elements of the independent set $\mathcal{C}$. This is a contradiction — unless w was in $\mathcal{B}$ to begin with. (Relations of the form "$w - w = 0$" don't count as nontrivial linear relations, since the vector w is repeated.)

Thus, $\mathcal{C} \subset \mathcal{B}$, so $\mathcal{B} = \mathcal{C}$. Hence, $\mathcal{B}$ is a maximal independent set. $\square$

Example. The ring

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. It inherits a norm from $\mathbb{C}$ given by

$$N\left(a + b\sqrt{-2}\right) = a^2 + 2b^2.$$

(Note that $|a + b\sqrt{-2}| = |a + b\sqrt{2}i| = a^2 + 2b^2$ as a complex number.)

$$N(xy) = N(x)N(y),$$

since this is true for the norm $|\cdot|$ for $\mathbb{C}$.

(a) Show that the units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

If $xy = 1$, then $N(x)N(y) = N(1) = 1$. Since $N(\cdot) \in \mathbb{Z}$, it follows that $N(x) = \pm 1$. Write $x = a + b\sqrt{-2}$. Then

$$1 = a^2 + 2b^2.$$

If $b \neq 0$, then $2b^2 \geq 2$ $\times$. Hence, $b = 0$, $1 = a^2$, and $a = \pm 1$. Thus, $x = \pm 1$. $\square$

(b) Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with $N(\cdot)$ as its valuation.

Write $x = a + b\sqrt{-2}$, $y = c + d\sqrt{-2}$, $x, y \neq 0$. Division of x by y is possible in $\mathbb{C}$:

$$\frac{x}{y} = e + f\sqrt{-2}, \qquad e, f \in \mathbb{Q}.$$

However, I need a quotient in $\mathbb{Z}[\sqrt{-2}]$.

Choose integers p and q such that

$$|p - e| \leq \frac{1}{2}, \qquad |q - f| \leq \frac{1}{2}.$$

$p + q\sqrt{-2}$ is the candidate for the quotient of x by y.

First,

$$|(e + f\sqrt{-2}) - (p + q\sqrt{-2})| = |(e - p) + (f - q)\sqrt{-2}| = (e - p)^2 + 2(f - q)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}.$$

Let $z = x - y(p + q\sqrt{-2})$. z will be the remainder; I must show that it has norm less than the norm of the divisor y.

$$N(z) = N\left(x - y(p + q\sqrt{-2})\right) = \left|y \cdot \left(\frac{x}{y} - (p + q\sqrt{-2})\right)\right| =$$

$$|y|\left|(e + f\sqrt{-2}) - (p + q\sqrt{-2})\right| \le N(y) \cdot \frac{3}{4} < N(y).$$

Hence, the division algorithm holds.

Finally, suppose $a + b\sqrt{-2}, c + d\sqrt{-2} \ne 0$. Then

$$N\left((a + b\sqrt{-2})(c + d\sqrt{-2})\right) = N(a + b\sqrt{-2})N(c + d\sqrt{-2}).$$

Since $N(c + d\sqrt{-2}) \ge 1$,

$$N\left((a + b\sqrt{-2})(c + d\sqrt{-2})\right) \ge N(a + b\sqrt{-2}).$$

It follows that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

Remark. It follows that $\mathbb{Z}[\sqrt{-2}]$ is a UFD. This is a special case of a famous problem.

Let d be an integer, and let $\mathbb{Q}(\sqrt{d})$ denote the field $\{s + t\sqrt{d} \mid s, t \in \mathbb{Q}\}$. The **integers** in $\mathbb{Q}(\sqrt{d})$ are:

- $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ if $d \ne 1 \bmod 4$.
- $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}, a, b$ both even or both odd$\}$ if $d = 1 \bmod 4$.

Consider the case $d < 0$. Gauss conjectured that the integers in $\mathbb{Q}(\sqrt{d})$ are a UFD exactly for d equal to

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

By the 1930's, the nine values above were known to give UFDs. Heilbronn and Linfoot proved that there were at most ten values which would produce UFDs. In 1966, Stark and Baker independently proved Gauss's conjecture using methods from complex analysis. □