Exercise 3.1.1. Which of the following subsets of the vector space of real $n \times n$ matrices is a subspace?

(a) symmetric matrices ($A = A^{\mathrm{t}}$)

(b) invertible matrices

(c) upper triangular matrices

(a) YES.

(b) NO. Note that 0_V is not invertible.

(c) YES.

Exercise 3.1.5. Prove that the classification of subspaces of $\mathbb{R}^3$ stated after (1.2) is complete.

Proof. Let $W \subset \mathbb{R}^3$ be a subspace.

- If $W = \{0\}$, we are in the trivial case.
- Suppose $W \neq \{0\}$. Then there exists some nonzero vector $v_1 \in W$. Since W is closed under scalar multiplication,
$$\{cv_1 : c \in \mathbb{R}\} \subset W,$$
which is precisely the line through the origin spanned by v_1. So if W contains nothing else, then W is a line.
- If W is not just a line, then there exists another vector $v_2 \in W$ that is not a scalar multiple of v_1. Then $\{c_1v_1 + c_2v_2 : c_1, c_2 \in \mathbb{R}\} \subset W$, i.e. the span of $\{v_1, v_2\}$. This is a plane through the origin.
- If W is not just a plane, then there exists $v_3 \in W$ that does not lie in the span of $\{v_1, v_2\}$. Then $\{c_1v_1 + c_2v_2 + c_3v_3 : c_1, c_2, c_3 \in \mathbb{R}\} = \mathbb{R}^3$. Hence $W = \mathbb{R}^3$.

Thus the only possibilities are $\{0\}$, a line through the origin, a plane through the origin, or all of $\mathbb{R}^3$.

$\square$

Exercise 3.2.1. Prove that the set of numbers of the form $a + b\sqrt{2}$, where a, b are rational numbers, is a field.

Proof. Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

- F is an abelian group under $+$: 0 is the identity, $-a - b\sqrt{2}$ is the inverse of $a + b\sqrt{2}$, and $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in F$.

- $F \setminus \{0\}$ is an abelian group under $\cdot$: 1 is the identity, $\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$ is the inverse of $a + b\sqrt{2}$, and $(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in F \setminus \{0\}$.
- The distributive law is inherited from $\mathbb{R}$.

$\square$

Exercise 3.2.7. Define homomorphism of fields, and prove that every homomorphism of fields is injective.

Proof. For 2 fields F, F', we say $f : F \to F'$ is a homomorphism if $f(a+b) = f(a)+f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in F$, and $f(a) = 0$ if and only if $a = 0$.

If f is not injective, there exist $a \neq b$ such that $f(a) = f(b)$, showing $f(a + (-b)) = 0$, which leads to a contradiction.

$\square$

Exercise 3.2.15. (a) By pairing elements with their inverses, prove that the product of all nonzero elements of a field F is -1.

(b) Let p be a prime number. Prove *Wilson's Theorem*:

$$(p-1)! \equiv -1 \pmod{p}.$$

(a) *Proof.* Note that equation $x^2 = 1$ can only have 2 solutions: $x = \pm 1$. This means by pairing elements with their inverses, only 1 and -1 will be paired with themselves, thus we have:

$$\left(\prod_{a \in F \setminus \{0,1,-1\}} a \right) = 1.$$

Hence, we know:

$$\left(\prod_{a \in F \setminus \{0\}} a \right) = 1 \cdot (-1) = -1.$$

$\square$

(b) Note that $\mathbb{Z}/p\mathbb{Z}$ is a field, we can conclude this result from (a).