The following problems come from section 7.1 of *Abstract Algebra* by Dummit and Foote.

3) Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.

Proof
Recall that a unit in a ring is one such that it has a multiplicative inverse. Let $u \in S$ be a unit. Then, there exists some $v \in S$ such that $uv = vu = 1$. Since $S \subset R$, it immediately follows that $u, v \in R$, implying that u is also a unit in R.

■

Converse: We provide the following counterexample to show that if u is a unit in R and u is an element of some subring of R then it does not necessarily follow that it is a unit in the subring. Consider the ring $\mathbb{Z}/5\mathbb{Z}$ with $u = \bar{2}$ and a subring $S = \{\bar{0}, \bar{2}, \bar{4}\}$. It is clear that $\bar{2} \cdot \bar{3} = \bar{1}$, but $\bar{3} \notin S$.

5) Decide which of the following (a)-(f) are subrings of $\mathbb{Q}$:

a) the set of all rational numbers with odd denominators (when written in lowest terms)

We have $R = \{a/b \mid \gcd(a, b) = 1 \text{ and } b \equiv 1 \pmod 2\}$. Then to prove this a subring of rational numbers, we need to prove this set is closed under addition and multiplication. It is trivial to see that R is an abelian additive group since $(R, +) \leq \mathbb{Q}$ and $\mathbb{Q}$ is an abelian group under addition. Thus,

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Notice that bd is odd, but we must check that if the numerator and denominator have common divisors that we are still left with an odd denominator after the rational number is written in lowest terms. This is simple to observe since $2 \nmid b$ and $2 \nmid d$ implies that $\gcd(ac, bd)$ and $\gcd(ad - bc, bd)$ cannot be even. Thus, converting the results to lowest terms we will retain an odd number in the denominator. Hence, R is a subring of $\mathbb{Q}$.

b) the set of all rational numbers with even denominators (when written in lowest terms)

We have $R = \{a/b \mid \gcd(a, b) = 1 \text{ and } b \equiv 0 \pmod 2\}$. Here, we have the same algebraic form for addition and multiplication of elements in R with b, d being even in this case. Observe that a and c must be odd, so ac. Thus, multiplication will always give an even number in the denominator since we only reduce by odd numbers. For addition, the largest even number in the numerator is $\gcd(b, d)$, whereas the largest even number in the denominator is $\gcd(b, d)^2$, so reducing by this and other common odd divisors of the numerator and denominator will still leave us with an even denominator since $\gcd(b, d)$ is even.

c) the set of nonnegative rational numbers

We have $R = \mathbb{Q}^+ \cup \{0\}$. This is not necessarily a subring since $(R, +)$ is not a subgroup of $\mathbb{Q}$. This is evident since say, for example, the additive inverse of $1/2$ (which is $-1/2$) is not in the set R

d) the set of squares of rational numbers

We have $R = \{a^2/b^2 \mid a/b \in \mathbb{Q}\}$. It is clear that this is not a subring since the set is not closed under addition. That is,

$$\frac{a^2}{b^2} - \frac{c^2}{d^2} = \frac{a^2d^2 - b^2c^2}{b^2d^2}$$

is not necessarily a square of a rational number. Take as an example adding $1/4$ and $1/9$. Then $a^2d^2 - b^2c^2 = 9 - 4 = 5$, which is not a perfect square (the denominator is 36 and $\gcd(5, 36) = 1$ so $5/36$ is reduced fully).

e) the set of all rational numbers with odd numerators (when written in lowest terms)

We have $R = \{a/b \mid \gcd(a, b) = 1 \text{ and } a \equiv 1 \pmod 2\}$. This is a ring, and the argument is similar to the case above where the denominator is odd, switching the roles of the denominator and numerator.

f) the set of all rational numbers with even numerators (when written in lowest terms)

We have $R = \{a/b \mid \gcd(a, b) = 1 \text{ and } a \equiv 0 \pmod 2\}$. This is a ring for similar reasons as in the case where the denominator is negative, effectively switching the roles of the denominator and numerator from above.

7) The *center* of a ring R is $\{z \in R | zr = rz \text{ for all } r \in R\}$ (i.e. is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

Proof
Obviously, 0 is in the center and if z is in the center, then $-z$ must be in the center since if $zr = rz$ then $-zr = -rz = r(-z)$. Finally, we see that addition is trivially associative, and multiplication is also clearly associative since it is in R. Additionally, since the elements in R satisfy the distribution laws, it immediately follows that the elements in the center do as well since they are in R.

Furthermore, if we impose that R is a division ring, then we claim that the center of R is a field. Since R is a division ring, then every nonzero element of R has a multiplicative inverse. Thus, since the center is by definition a commutative ring and it retains the property of being a division ring from R, it follows that it is a field.

■

11) Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

Proof
Since R is an integral domain it contains no zero divisors. Hence if $x^2 = 1$, then $x^2 - 1 = (x-1)(x+1) = 0$. By the cancellation laws and since R is an integral domain, we must have that $x - 1 = 0$ or $x + 1 = 0$, implying $x = \pm 1$.

■

13) An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.

a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.

Proof
Notice that $(ab)^k = a^k b^k = nb^{k-1}$, so $\overline{ab}^k = \bar{n}\bar{b}^{k-1} = \bar{0}\bar{b}^{k-1} = \bar{0}$.

■

b) If $a \in \mathbb{Z}$, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent iff every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.

Proof
($\Longrightarrow$) We have that $\exists m \in \mathbb{Z}^+$, $\bar{a}^m = \bar{0}$ and that $p \mid n$ is prime. Thus, it follows that $a^m \equiv 0 \mod n$ or $a^m = nk$ for some integer k. Hence, $n = pl$, implying that $a^m = plk$ and $p \mid a^m$. Thus, it follows that $p \mid a$ (easily proven from the fundamental theorem of arithmetic).

($\Longleftarrow$) Suppose that every prime divisor of n is also a prime divisor of a. That is, if p is prime and $p \mid n$ then $p \mid a$. Hence, by the fundamental theorem of arithmetic we can write $n = p_1^{s_1} \dots p_k^{s_k}$ and $a = p_1^{t_1} \dots p_k^{t_k} z$, where z is an integer which is not divisible by any of the primes which divide n. Define $m = \min\{l \in \mathbb{Z}^+ \mid lt_i - s_i \text{ for } i = 1, \dots, k\}$. Observe that $a^m = p_1^{mt_1} \dots p_k^{mt_k} z^m$. It is clear then that $a^m = nx$, where x is some integer. Thus, $\bar{a}^m = \bar{n}\bar{x} = \bar{0}\bar{x} = \bar{0}$.

■

Note: A particularly nice choice of m may be $m = s_1 \dots s_k$. It is then clear that $a^m \mid n$ without resorting to set notations, etc. (although these choices are no less valid).

The nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are those which are even or divisible by three since $72 = 2^3 3^2$.

14) Let x be a nilpotent element of the commutative ring R

a) Prove that x is either zero or a zero divisor.

Proof
Since x is nilpotent, there exists a positive integer such that $x^m = 0$. Further suppose

that m is the smallest such integer satisfying this. Consider the following cases. First, if $x = 0$ then we are done. Next, if $x \neq 0$, then $xx^{m-1} = x^{m-1}x = 0$, implying that x is a zero divisor since $x^{m-1} \neq 0$.

■

b) Prove that rx is nilpotent for all $r \in R$.

Proof
Suppose that $x^m = 0$ for some $m \in \mathbb{Z}^+$. Observe that $(rx)^m = r^m x^m = r^m 0 = 0$.

■

c) Prove that $1 + x$ is a unit in R.

Proof
Consider the product

$$(1+x)\sum_{n=0}^{m-1}(-x)^n = \sum_{n=0}^{m-1}(-x)^n + \sum_{n=0}^{m-1}(-x)^{n+1}$$

We may compare powers of x and notice that only the first term in the first sum survives (one may also shift indices in the first sum $n+1 \to n$) which is just 1. Thus, $1 + x$ is a unit.

■

d) Deduce that the sum of a nilpotent element and a unit is a unit.

Proof
Let a be a nilpotent element of R where $a^m = 0$ and u be a unit of R such that $uv = 1$, where $v \in R$. Then we show that $a + u$ is a unit.

$$\begin{aligned}(a+u)v\sum_{n=0}^{m-1}(-va)^n &= v\left[\sum_{n=0}^{m-2}(-v)^n(a)^{n+1} + \sum_{n=0}^{m-1}u(-v)^n(a)^n\right] \\ &= v\left[\sum_{n=1}^{m-1}(-v)^{n-1}(a)^n + u - \sum_{n=1}^{m-1}(-v)^{n-1}(a)^n\right] \\ &= vu = u\end{aligned}$$

■

*It is important to note that the ring must be commutative. In the proofs above, commutativity is implicitly used as opposed to being explicitly referenced.

15) A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

Proof
Notice that $(2a)^2 = a^2 + a + a + a^2 = a + a$ or $a = -a$ for all $a \in R$. Observe that $(a+b)^2 = a+b = a^2+ab+ba+b^2 = a+ab+ba+b$. Thus, $ab+ba = 0$ or $ab = -ba = ba$.

■

17) Let R and S be rings. Prove that the direct product $R \times S$ is commitative iff both R and S are commutative. Prove that $R \times S$ has an identity iff both R and S have identities.

Proof
($\Longrightarrow$) Suppose that $R \times S$ is commutative, then $(r_1, s_1)(r_2, s_2) = (r_2, s_2)(r_1, s_1)$. Comparing by components we have $r_1 r_2 = r_2 r_1$ and $s_1 s_2 = s_2 s_1$ or that R and S are commutative.

($\Longleftarrow$) Suppose that R and S are commutative. Then, $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_2) = (r_2, s_2)(r_1, s_1)$. Hence, $R \times S$ is commutative.

■

Proof
($\Longleftarrow$) Suppose that R and S have identities 1_R and 1_S, respectively. Then $R \times S$ has the identity $(1_R, 1_S)$ since $(1_R, 1_S)(r, s) = (1_R r, 1_S s) = (r, s)$.

($\Longrightarrow$) Suppose that $R \times S$ has identity $(1_R, 1_S)$. Then, $1_R \in R$ and $1_S \in S$ and for any $(r, s) \in R \times S$ we have $(1_R, 1_S)$ since $(1_R, 1_S)(r, s) = (1_R r, 1_S s) = (r, s)$. Hence $1_R r = r$ and $1_S s = s$, implying that 1_R and 1_S are the identities for R and S, respectively.

■

20) Let R be a collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_3, a_3, \ldots$ where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of $\mathbb{Z}$). Prove that R is a ring under component wise addition and multiplication which does not have an identity.

Proof
If we define addition as $(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$ and multiplication as $(a_1, a_2, a_3, \ldots)(b_1, b_2, b_3, \ldots) = (a_1 b_1, a_2 b_2, a_3 b_3, \ldots)$. Since the integers form a ring it is clear that multiplication is associative and the distribution laws follow when component-wise addition and multiplication is assumed. Additionally, it is clear that this is an abelian additive group with zero being the sequence $(0, 0, 0, \ldots)$, the inverse being $(-a_1, -a_2, -a_3, \ldots)$, and associativity follows from integer addition being associative. Thus, this is a ring.

We show now that this ring cannot have an identity. Suppose that it does: $(1_1, 1_2, 1_3, \ldots)$. Then, $(a_1, a_2, a_3, \ldots)(1_1, 1_2, 1_3, \ldots) = (a_1, a_2, a_3, \ldots)$. Recall that each element must have only finitely many sequence elements which are nonzero. Thus, we may pick a sequence such that $1_i = 0$ but $a_i \neq 0$. Then, $a_i 1_i = 0$, which is not a_i. This implies that no choice of an element gives an identity.

■