Exercises 18

⑦ Yes, a ring. We already know $n\mathbb{Z}$ is an abelian gp, & we know $\mathbb{Z}$ is a ring with respect to the same operations, so we need only show $n\mathbb{Z}$ is closed under $\cdot$ (i.e., it is a subring of $\mathbb{Z}$). Let $nx, ny \in n\mathbb{Z}$. Then $(nx)(ny) = n(nxy)$. Since $nxy \in \mathbb{Z}$, $n(nxy) \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is a ring. (unless $n = \pm 1$)
It is commutative b/c $\mathbb{Z}$ is, but it does not have unity; suppose $\exists nx \in n\mathbb{Z}$ s.t. $(nx)(ny) = ny \ \forall ny \in n\mathbb{Z}$. Then (by using the ring structure of $\mathbb{Z}$), $nx = 1$, so $x = n^{-1}$ (the multiplicative inverse). But if $n \neq \pm 1$, then $x \notin \mathbb{Z}$, which is a contradiction.
It is not a field: $n \in n\mathbb{Z}$, but if $n \neq \pm 1$, then $n^{-1} \notin \mathbb{Z}$, so $n^{-1} \notin n\mathbb{Z}$.

⑨ $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ is a ring b/c $\mathbb{Z}$ is & the direct product of rings is a ring.
It is commutative, b/c $\mathbb{Z}$ is, & unity is $(1,1)$
It is not a field, b/c $(2,2)$ has no multiplicative inverse.

⑩ $(2\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ is a ring, b/c $2\mathbb{Z}$ & $\mathbb{Z}$ are rings, & the direct product of rings is a ring. It is commutative because $2\mathbb{Z}$ & $\mathbb{Z}$ are. It does not have unity b/c $2\mathbb{Z}$ doesn't (and so there is no elt $(a,b) \in 2\mathbb{Z} \times \mathbb{Z}$ s.t. $(a,b)\cdot(n,0) = (n,0) \ \forall n \in 2\mathbb{Z}$.
It is not a field, because $(0,2)$ has no multiplicative inverse (and because it does not have unity).

⑪ $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. R is a ring: $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + b\sqrt{2}c + b\sqrt{2}d\sqrt{2} = ac + 2bd + (ad + bc)\sqrt{2} \in R$, so it is closed under $\cdot$, it is an abel. gp under $+$. Assoc. of $\cdot$ & distributive laws follow from the fact that $\mathbb{R}$ is a ring.
- R is commutative, b/c $\mathbb{Z}$ (& $\mathbb{R}$) are.
- R has unity: $1_R = 1 + 0\sqrt{2} = 1$
- R is not a field: $2 + 0\sqrt{2} = 2$ is not a unit (neither is $\sqrt{2}$)

⑫ $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a ring. The proof that it is closed is the same as in #11. R is commutative b/c $\mathbb{R}$ is ($\because R \subseteq \mathbb{R}$). R has unity: $1_R = 1 + 0\sqrt{2}$
R is a field: let $a + b\sqrt{2} \in \mathbb{Q}$. Then

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in \mathbb{Q}}\sqrt{2} \in R.$$

⑳ $M_2(\mathbb{Z}_2)$
(a) Order is $2^4 = 16$: There are 2 choices (0 or 1) for each of the 4 entries of the matrix.
(b) Units are $\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}\right\}$ (these are the matrices w/ non-zero determinant.

㉛ In $\mathbb{Z}_6$, $\bar{2}\cdot\bar{3} = \bar{0}$, but $\bar{2} \neq \bar{0}$ & $\bar{3} \neq \bar{0}$.

㉜ Here's one example: $S = \{\bar{0}, \bar{3}\} \leq \mathbb{Z}_6$. S is a subring: it is an abelian gp under $+$ & is closed under $\cdot$. $1_S = \bar{3}$: $\bar{3}\cdot\bar{0} = \bar{0}$, $\bar{3}\cdot\bar{3} = \bar{3}$
However $1_{\mathbb{Z}_6} = \bar{1} \neq \bar{3}$.

(37) Let $U = \{x \in R \mid x \text{ is a unit}\}$.
- Closure: let $x, y \in U$. Then $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1_R x^{-1} = x \cdot x^{-1} = 1_R$, so $y^{-1}x^{-1} = (xy)^{-1}$. Since $y^{-1}, x^{-1} \in R$, & R is closed under $\cdot$, $y^{-1}x^{-1} \in R$. Thus xy is a unit, so $xy \in U$.
- Assoc: Follows b/c $(R, \cdot)$ is assoc. (part of the def. of a ring)
- Identity: Let $1 \in R$ be unity. $1 \cdot 1 = 1$, so 1 is a unit & thus $1 \in U$. $\forall x \in U$, $1 \cdot x = x = x \cdot 1$, so 1 is the identity of U.
- Inverses: Let $x \in U$. Then $xx^{-1} = 1$ in R, so x^{-1} is a unit, as well, & thus $x^{-1} \in U$.

Therefore, $(U, \cdot)$ is a gp.

(39)
- Mult. is assoc: $\forall a, b, c \in R$, $(ab) \cdot c = 0c = 0 = a0 = a(bc)$ ✓
- Distrib. prop: $\forall a, b, c \in R$, $a \cdot (b+c) = 0 = 0 + 0 = ab + ac$, & similarly for right distributivity.

Thus R is a ring.

(42) Let $(F, +, \cdot)$ be a field, 1_F unity in F, & let $F' \leq F$ be a subfield. Let $x \in F'$ w/ $x \neq 0$. Then since F' is a subfield of F, $x^{-1} \in F$. Moreover, F' is closed under $\cdot$, so $1_F = xx^{-1} \in F'$. Let $y \in F'$. Then $y 1_F = y$, so 1_F is unity in F'!

b/c these are also elts of F, where 1_F is unity.

(44) (a) Let $I = \{a \in R \mid a^2 = a\}$, & suppose $a, b \in I$.
Then $(ab)^2 = abab = a^2 b^2 = ab \Rightarrow ab \in I$.
(R comm.)

(b) idempotents in $\mathbb{Z}_6$: 1, 3, 4, 0
idempotents in $\mathbb{Z}_{12}$: 1, 4, 9, 0

So, the idempotents in $\mathbb{Z}_6 \times \mathbb{Z}_{12}$ are
$\{(1,1), (1,4), (1,9), (3,1), (3,4), (3,9), (4,1), (4,4), (4,9),$
$(0,0), (0,1), (0,4), (0,9), (1,0), (3,0), (4,0)\}$

(46) Let R be a commutative ring & let $a, b \in R$ be nilpotent elts. Then $\exists n, m \in \mathbb{Z}^+$ s.t. $a^n = 0$ & $b^m = 0$.
Then $(a+b)^{n+m} = a^{n+m} + \binom{n+m}{1} a^{n+m-1} b + \cdots + \binom{n+m}{i} a^{n+m-i} b^i + \cdots + b^{n+m}$.
In every term, either $n+m-i \geq n$ or $i \geq m$. In the first case, $a^{n+m-i} = a^n a^{m-i} = 0\, a^{m-i} = 0$, & in the second case, $b^i = b^m b^{i-m} = 0 b^{i-m} = 0$
Thus there is a factor of 0 in each term, so $(a+b)^{n+m} = 0$, & $a+b$ is nilpotent.