Exercises 27:

(8) prime and max'l: (2), (3)

(4) ideals in $\mathbb{Z}_2 \times \mathbb{Z}_4$ | Quotient

$(0)\times(0)$	$\mathbb{Z}_2 \times \mathbb{Z}_4$
$(0)\times(2)$	$\mathbb{Z}_2 \times \mathbb{Z}_2$
$(0)\times(1)$	$\mathbb{Z}_2$ field & int. dom.
$(1)\times(0)$	$\mathbb{Z}_4$
$(1)\times(2)$	$\mathbb{Z}_2$ field & int. dom
$(1)\times(1)$	$\{0\}$

So, the prime & max'l ideals are $(0)\times(1)$ & $(1)\times(2)$.

(5) $\mathbb{Z}_3[x]/(x^2+c)$ is a field $\Leftrightarrow$ x^2+c is irred. over $\mathbb{Z}_3$. x^2+c is a quadratic, so we can check roots:

$c=0$: $x^2 = (x)(x)$, not irred.

$c=1$: x^2+1 irred ($0^2+1=1$, $1^2+1=2$, $2^2+1=2$)

$c=2$: x^2+2 red: $1^2+2=0$, so there is a linear factor of $x-1$.

Thus $\mathbb{Z}_3[x]/(x^2+c)$ is a field $\Leftrightarrow$ $c=1$.

(19) x^2-6x+6 is irreducible by Eisenstein with $p=2$. Therefore (x^2-6x+6) is maximal (by thm in book), & so $\mathbb{Q}[x]/(x^2-6x+6)$ is a field.

(24) Let R be a finite commutative ring w/ unity, & let $I \subseteq R$ be a prime ideal. Then R/I is an integral domain, and since R is finite, so is R/I. Since every finite integral domain is a field, R/I is a field. Therefore, I is maximal.

(30) Let F be a field & let I be a proper, non-triv. prime ideal of $F[x]$. Since our ideal in $F[x]$ is principal, $I=(f(x))$ for some $f(x) \in F[x]$. I is maximal $\Leftrightarrow$ $f(x)$ is irreducible (this is a thm in the book). Suppose $f(x) = a(x)b(x)$, where $a(x), b(x) \in F[x]$ & $\deg a(x), \deg b(x) < \deg f(x)$. Then $a(x)b(x) \in I$, & since I is prime, $a(x) \in I$ or $b(x) \in I$. Without loss of generality, assume $a(x) \in I$. Then $a(x) = f(x)g(x)$ for some $g(x) \in F[x]$. Since F is a field, $\deg a(x) = \deg f(x) \deg g(x) \geq \deg f(x)$, a contradiction. Thus $f(x)$ is irreducible & so I is a maximal ideal.

(34) (a) We first show $A+B$ is a subgp of R:

- closure under $+$: let $a+b, c+d \in A+B$. Then $(a+b)+(c+d) = (a+c)+(b+d) \in A+B$ b/c A & B are closed under $+$.
- identity: A, B are subgps, so $0 \in A$ & $0 \in B$. Thus $0 = 0+0 \in A+B$.
- inverses: Let $a+b \in A+B$. Then $-a \in A$ & $-b \in B$, as these are both subgps, so $-(a+b) = -a+(-b) \in A+B$.

Thus $A+B$ is a subgp of R. To show it is an ideal, let $r \in R$ & $a+b \in A+B$. Then

$r(a+b) = ra+rb \in A+B$ b/c A & B are ideals so $ra \in A$ & $rb \in B$.

Similarly, $(a+b)r = ar+br \in A+B$.

Therefore $A+B$ is an ideal.

(b) $A \subseteq A+B$: Let $a \in A$. Then $a = a+0 \in A+B$ since $0 \in B$.
$B \subseteq A+B$: Let $b \in B$. Then $b = 0+b \in A+B$ since $0 \in A$.

(35) (a) We first show AB is a subgp of R:
- closure under +: Let $\sum_{i=1}^{n} a_i b_i$, $\sum_{j=1}^{m} c_i d_i \in AB$

Then $\sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} c_i d_i = \sum_{k=1}^{n+m} e_k f_k$, where $e_k = \begin{cases} a_i & \text{if } 1 \le k \le n \\ c_i & \text{if } n+1 \le k \le n+m \end{cases}$

& $f_k = \begin{cases} b_i & \text{if } 1 \le k \le n \\ d_i & \text{if } n+1 \le k \le n+m \end{cases}$. Thus, $e_k \in A$ & $f_k \in B$ $\forall k$, so this sum is in AB.

- Identity: $0 \in A$ & $0 \in B$, so $0 = 0 \cdot 0 \in AB$.
- Inverses: Let $\sum_{i=1}^{n} a_i b_i \in AB$. Then $-\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (-a_i) b_i$. Since $-a_i \in A$ b/c A is a subgp, this sum is in AB.

Thus, AB is a subgp of R. To show AB is an ideal, let $r \in R$ and $\sum_{i=1}^{n} a_i b_i \in AB$. Then $r \cdot \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (r a_i) b_i \in AB$, since A is an ideal & so $r a_i \in A$ $\forall i$. Similarly, $(\sum_{i=1}^{n} a_i b_i) \cdot r = \sum_{i=1}^{n} a_i (b_i r) \in AB$ since B is an ideal & so $b_i r \in B$ $\forall i$.

Therefore, AB is an ideal of R.

(b) Let $\sum_{i=1}^{n} a_i b_i \in AB$. Since A is an ideal, $a_i b_i \in A$ $\forall i$, & since A is also a subring & so closed under +, $\sum_{i=1}^{n} a_i b_i \in A$. Similarly, B is an ideal & so a subring, & thus $\sum_{i=1}^{n} a_i b_i \in B$.
Therefore, $AB \subseteq A \cap B$.

(36) We first show $A:B$ is a subgp of R.
- closure under +: Let $r, s \in A:B$. Then $rb \in A$ & $sb \in A$ $\forall b \in B$. $(r+s)b = rb + sb \in A$ as A is a subgp of R & so closed under +. Thus $r+s \in A:B$.
- Identity: A is a subgp, so $0 \in A$. Since $\forall b \in B$, $0b = 0 \in A$, $0 \in A:B$.
- Inverses: Let $r \in A:B$. Then $\forall b \in B$, $rb \in A$. For any $b \in B$, $(-r)b = -(rb) \in A$ b/c A is a subgp & so closed under additive inverses.

Thus $A:B$ is a subgp of R. To show $A:B$ is an ideal, let $r \in R$ & $x \in A:B$. Then $\forall b \in B$, $xb \in A$.
For any $b \in B$, $(rx)b = r(xb) \in A$ because A is an ideal.

Since R is a commutative ring, this suffices to show $A:B$ is an ideal.

(37) We first show S is a subgp of $M_2(F)$.
- closure under +: Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in S$.

Then $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix} \in S$.

- Identity: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$

• Inverses: Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in S$. Then $-\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} \in S$.

Thus S is a subgp. To show S is a subring, we show it is closed under $\cdot$: Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in S$.

Then $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in S$

Thus S is a subring. To show S is a right ideal, let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in S$ & $\begin{pmatrix} c & d \\ e & f \end{pmatrix} \in M_2(F)$.

Then $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac+be & ad+bf \\ 0 & 0 \end{pmatrix} \in S$. Thus S is a right ideal.

To show S is <u>not</u> a left ideal, consider $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(F)$, where 1 is unity in F. Then $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \notin S$.

Thus S is not a left ideal.

(38) The best way to do this problem is by brute force. Suppose I is a nontrivial ideal of $M_2(\mathbb{Z}_2)$. Then I contains a non-zero elt A. We will show that I must be all of $M_2(\mathbb{Z}_2)$, which will prove the result.

First, notice that if A is a unit, then $I = M_2(\mathbb{Z}_2)$. The elts of $M_2(\mathbb{Z}_2)$ which are units are those with non-zero determinant, i.e., the matrices of rank 2. Thus we may assume A has rank 1. The rank 1 matrices in $M_2(\mathbb{Z}_2)$ are:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

• Suppose $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Then $A + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

and since $A \in I$ & I is an ideal, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$. Since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a unit (in fact, unity), $I = M_2(\mathbb{Z}_2)$.

• Suppose $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $A\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

& so $I = M_2(\mathbb{Z}_2)$, as above.

• Suppose $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

Then $A\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$, and we showed above that this implies that $I = M_2(\mathbb{Z}_2)$.

• Suppose $A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$. Then $A\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I$,

and we also showed above that this implies that $I = M_2(\mathbb{Z}_2)$.

Thus if I is a nontrivial ideal, then $I = M_2(\mathbb{Z}_2)$. Therefore, $M_2(\mathbb{Z}_2)$ is simple.

Exercises 29

① $x = 1+\sqrt{2}$

$(x-1)^2 = 2$

$x^2 - 2x - 1 = 0$.

Let $f(x) = x^2 - 2x - 1 \in \mathbb{Q}[x]$. Then $f(1+\sqrt{2}) = 0$, so $1+\sqrt{2}$ is algebraic over $\mathbb{Q}$.

② $x = \sqrt{2}+\sqrt{3}$

$x^2 = 2 + 2\sqrt{6} + 3$

$(x^2 - 5)^2 = 24$

Let $f(x) = x^4 - 10x^2 - 1$. Then $f(\sqrt{2}+\sqrt{3}) = 0$, so $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$.

③ $x = 1+i$

$(x-1)^2 = -1$

Let $f(x) = x^2 - 2x + 2$. Then $f(1+i) = 0$, so $1+i$ is algebraic over $\mathbb{Q}$.

Additional Exercise:

① Let F be a field, & consider the subset $\{n \cdot 1 \mid n \in \mathbb{Z}\} = S$

S is a subring of F:

- S is a subgp:
  - closure under +: Let $n\cdot 1, m\cdot 1 \in S$. Then $n\cdot 1 + m\cdot 1 = (n+m)\cdot 1 \in S$ because $n+m \in \mathbb{Z}$.
  - Identity: $0 = 0\cdot 1 \in S$
  - Inverses: Let $n\cdot 1 \in S$. Then $-(n\cdot 1) = (-n)\cdot 1 \in S$ since $-n \in \mathbb{Z}$.

  Therefore, S is a subgp of F.
- Let $n\cdot 1, m\cdot 1 \in S$, then $(n\cdot 1)(m\cdot 1) = (nm)\cdot 1 \in S$. Therefore S is closed under multiplication, & so S is a subring of F.

We now show that S is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Q}$, depending on the characteristic of F.

- If char $F = 0$:

  Let $\varphi: S \to \mathbb{Z}$ be defined by $\varphi(n\cdot 1) = n$.

  Then $\varphi(n\cdot 1 + m\cdot 1) = n+m = \varphi(n\cdot 1) + \varphi(m\cdot 1) \Rightarrow \varphi$ a gp hom.

  $\varphi((n\cdot 1)(m\cdot 1)) = \varphi((nm)\cdot 1) = nm = \varphi(n\cdot 1)\varphi(m\cdot 1) \Rightarrow \varphi$ a ring hom.

  - φ is clearly an isomorphism.

  Thus F has a subring isomorphic to $\mathbb{Z}$. Since F is a field, F must contain the field of fractions of $\mathbb{Z}$, which is isomorphic to $\mathbb{Q}$. Thus F has a subfield isomorphic to $\mathbb{Q}$.

- If $\operatorname{char} F \neq 0$, then you've shown $\operatorname{char} F = p$ for some prime p. (you proved this in HW for any integral domain).
  Define $\varphi: S \to \mathbb{Z}_p$ the same way. Same pf holds that φ a ring hom.
  - φ is injective: If $\varphi(n\cdot 1) = \varphi(m\cdot 1)$, then $n \equiv m \pmod p$, so $\exists q_1, q_2, r \in \mathbb{Z}$ s.t. $n = q_1 p + r$, $m = q_2 p + r$.
    So $n\cdot 1 = (q_1 p + r)\cdot 1 = (q_1 p)\cdot 1 + r\cdot 1 = p(q_1 \cdot 1) + r\cdot 1 = 0 + r\cdot 1 = r\cdot 1$ (since $\operatorname{char} F = p$).
    Similarly, $m\cdot 1 = r\cdot 1$.
    Thus $n\cdot 1 = m\cdot 1$. ✓
  - φ is clearly surj.

Therefore, F has a subfield isomorphic to $\mathbb{Z}_p$.