Ch19

B2

The following function is a homomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_3$

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

The kernel of f is $\{0, 3\} = \langle 3 \rangle$. Thus

$$\mathbb{Z}_6 \xrightarrow[\langle 3 \rangle]{} \mathbb{Z}_3$$

It follows by the FHT that $\mathbb{Z}_3 \cong \mathbb{Z}_6/\langle 3 \rangle$

B4

The following function is a homomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_2$ to $\mathbb{Z}_2$

$$f = \begin{pmatrix} (0,0) & (0,1) & (1,0) & (1,1) \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The kernel of f is $\{(0,0), (0,1)\} = K$. Thus.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow[K]{} \mathbb{Z}_2$$

2/2 It follows by the FHT that $\mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2/K$.

F1

Let $a, b \in A$. then $ab = ba$. then

$(J+a)(J+b) = J+ab = J+ba = (J+b)(J+a)$ is commutative

Let $J+x$ be the unity of A/J then.

$(J+x)(J+a) = J+ax = J+a \Rightarrow x=1$. x is the unity of A

So $J+1$ is the unity of A/J.

$(A/J, +)$ abelian:

$(J+a)+(J+b) = J+(a+b) = J+(b+a) = (J+b)+(J+a)$.

$(A/J, \cdot)$ associative:

$(J+a)[(J+b)(J+c)] = (J+a)(J+(bc)) = J+(abc) =$

$= (J+(ab))(J+c) = [(J+a)(J+b)](J+c)$

$(A/J, \cdot)$ distributive:

$(J+a)((J+b)+(J+c)) = (J+a)(J+(b+c)) = J+a(b+c) = J+(ab+ac)$

$= (J+ab) + (J+ac) = (J+a)(J+b) + (J+a)(J+c)$.

F2.

A/J is commutative ring with unity $J+1$.

$(J+a)(J+b) = J \Leftrightarrow ab \in J \Leftrightarrow a \in J$ or $b \in J$.

$\Leftrightarrow J+a = J$ or $J+b = J$

So A/J does not have divisors of zero and

2/2 hence is an integral domain and vice versa

F3

Let J be a maximal ideal of A. By the fact. A/J is a field. Since field is integral domain So A/J is an integral domain. By F2, J is a prime ideal

F4

By Theorem 3. $f: A \to A/J$ is a homormophism. let K be the kernel of f. then $A/K \cong A/J$. By Ch18 ExI2, since A/J is a field, K is a maximal ideal. since $A/K \cong A/J$, $J = K$. is also a maximal ideal.

Ch20. A3.

$char(A) = 3$. Since $5a = 0$. $3 \mid 5$ doesn't hold then $a = 0$. 2/2

A6

Let $p = char(A)$ then $(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$

$\Rightarrow$ ~~...~~ $p \mid 2$. since p is prime $p = 2$

B1

$ord(A) = n$. $char(A) = q$, $q \cdot a = 0$ $\forall a \in A$.

also $n \cdot a = 0$ $\forall a \in A$.

let $n = pq + r$ where $0 \le r < q$

then $na = p(qa) + ra$. $\Rightarrow 0 = 0 + ra \Rightarrow ra = 0$. $\forall a \in A$.

Since $r < q$. then $r = 0$. so $n = pq \Rightarrow q \mid n$.

B3 which theorem you used? 2/2 1.5/2

$ord(A) = p^m$. $char(A) \mid p^m$ and $char(A)$ is prime.

since $p^2, p^3, \dots p^m$ are not prime, $char(A) = p$

E4

$f(a) = a^p$ $f(b) = b^p$ ~~$f(ab) = (ab)^p$~~ Since A is commutative $f(ab) = (ab)^p = (a^p)(b^p) = f(a) f(b)$.

$f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$ by theorem 3

so f is a homomorphism from A to A. 2/2

F2

By E4, we know $f(a) = a^p$ is homomorphism.

By theorem 4. $\forall a \in A$ a is invertible

List elements of the finite field: $0, 1, a_1 \cdots a_{n-2}$.

there are n elements in domain. for $1 \le i \le n-2$ the product $a_i 0^p, a_i 1^p, a_i a_1^p \cdots a_i a_{n-2}^p$ are all distinct.

but there are exactly n element in domain. so element in domain is equal to one of these product.

so f is injective. $\Rightarrow f$ is automorphism

F3

Assume the root of $x^p - \alpha$ is β. then

$(x-\beta)^p = x^p - \beta^p = x^p - \alpha$.

In finite field F. by F2. $\alpha \mapsto \alpha^p$ is automorphism

so β is the p-th root.

Ch21 C5.

$S_1 : n=1 \quad 1 = \frac{1\times 2\times 3}{6} = 1$ hold.

Assume $S_k = \sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$ is true.

then $S_{k+1} = S_k + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$$= \frac{1}{6}(2k^3+3k^2+k) + \frac{1}{6}(6k^2+12k+6).$$

$$= \frac{1}{6}(2k^3+9k^2+13k+6).$$

$$= \frac{1}{6}[(k+1)(k+2)(2k+3)] \quad \text{hold.}$$

Therefore $S_n : \sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$. is true

C6

2/2

$S_1 : n=1 \quad 1^3 = \frac{1}{4}\times 1^2 \times 2^2 = 1$. hold.

Assume $S_k : \sum_{i=1}^{k} i^3 = \frac{1}{4}k^2(k+1)^2$ is true.

then $S_{k+1} = S_k + (k+1)^3 = \frac{1}{4}k^2(k+1)^2 + (k+1)^3$

$$= (k+1)^2(\tfrac{1}{4}k^2 + k+1) = \tfrac{1}{4}(k+1)^2(k+2)^2 \quad \text{hold}$$

Therefore $S_n = \sum_{i=1}^{n} i^3 = \frac{1}{4}n^2(n+1)^2$ is true

Ch22 F1

let $c = \mathrm{lcm}(a.b)$, $\langle c\rangle$ is the generator of the set.
It is obvious the $\langle c\rangle$ is a ring. Below is prove of ideal.

~~$\langle c\rangle$ is subring~~
~~Closed on substraction~~.

① let $y_1 = cx_1$. $y_2 = cx_2$ for some $x_1 x_2 \in \mathbb{Z}$. $y_1 \cdot y_2 \in \langle c\rangle$
$y_1 - y_2 = (x_1 - x_2)c$. $x_1 - x_2 \in \mathbb{Z}$. $\Rightarrow y_1 - y_2 \in \langle c\rangle$.
② $y_1 y_2 = c(cx_1x_2)$. $cx_1x_2 \in \mathbb{Z}$. $y_1y_2 \in \langle c\rangle$.
③ for $\forall k \in \langle c\rangle$. $\forall j \in \mathbb{Z}$ $jk = jnc \in \langle c\rangle$ for some n
So $\langle c\rangle$ is ideal of $\mathbb{Z}$.

F2.

~~By definition, we have a|c b|c~~ Since the set of the multiple of a and b is generated by $\langle c\rangle$ So the lcm of a and b will be $\min(\langle c\rangle)$.

2/2

F4

Since $\gcd(a.b) \cdot \mathrm{lcm}(a.b) = ab$.

$$\mathrm{lcm}(ab) = \frac{ab}{\gcd(a.b)} = \frac{ab_1c_2}{c} = a_1b_1c.$$

G2.

Assume a prime ideal $\langle p\rangle$ of $\mathbb{Z}$. Then If $\langle p\rangle \subseteq \langle a\rangle$ then either ~~p=1 or p=a~~ $a=1$ or $a=p$.
Since p is prime and is relative prime to any other integer. since $\langle p\rangle \neq \langle a\rangle \Rightarrow a=1$. $1 \in \langle a\rangle$.
$\langle p\rangle \subset \langle 1\rangle$. so $\langle p\rangle$ is a maximal ideal

2/2