Assignment 12

Problem 1 (6..48)

Exercise 6.48 - Using the function theorem of finite group (either form), give short and simple proof of Theorem 6.41 and 6.42

Theorem 6.41. If abelian group G has non-zero exponent m, then G contains an element of order m. In paticular, a finite abelian group is cyclic if and only if its order equals its exponent

Using the theorem 6.45 which saying a finite abelian group is isomorphic to a direct product of cyclic group $\mathbb{Z}_{m_1} \times \cdots \mathbb{Z}_{m_t}$, m_t is the exponents

the direct product of cyclic groups $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$, m_t is te exponents of the group and it is the order of this cyclic groups. $m_1 \sim m_t$ are uniquely determing. so m is a non-zero exponent.

For Theorem 6.42 : Let G be a finite abelian group of order n. If p is a prime dividing n, then G contains an element of order p.

Using the fundamental theorem of finite abelian groups, theorem 6.44. : A finite abelian group (more than one element) is isomorphic to a direct product of cyclic groups

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}},$$ where the p_i's are primes (not necessarily distinct) and the e_i's are positive integers. This direct product of cyclic groups is unique up to the order of the factors.

So a finite abelian groups of order n. from the theorm n is composite with prime numbers $\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}$ can have cycle of of each primes $p_1 \cdots p_r$ since tey all divide n.

Assignment 12

Problem 1 (7.3)

Let R be a ring, and let $a, b \in R$ such that $ab \neq 0$. Show that ab is a zero divisor if and only if a is a zero divisor or b is a zero divisor

From the definition of the question we have $ab \neq 0$. so we have $a \neq 0, b \neq 0$ a, b are non-zero elements.

If ab is a zero divisor then let's say the other zero divisor part of ab is c, $c \in R$ so $(ab)c = 0$ c is also non-zero elemene. In order to $(ab)c$ be a zero divisor, either $ac = 0$ or $bc = 0$. When $ac = 0$ $(ab)c = (a0)b = 0 \cdot b = 0$ due to associative It also work same for when $bc = 0$

Converse part.
If a or b is a zero divisor, either one has zero divisor pair c, ($ac = 0$) or ($bc = 0$) so ab would also be an zero divisor since $abc = 0$ by associative Rule. $(ac)b = 0$ $ac = 0$, or $a(bc) = a \cdot 0 = 0$.

non zero, $\in R$

Problem 2 (7.13)

Show that the set $\mathbb{Q}[i]$ of complex number of the form $a+bi$, with $a, b \in \mathbb{Q}$, is a subfield of $\mathbb{C}$.

The definition of subfield is when There is a field F, F' is a subring of F and F' is a subfield itself

Since $\mathbb{Q}[i]$ is the set of complex number of the form $a+bi$, $a, b \in \mathbb{Q}$. $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$ because $1_R \in \mathbb{Q}[i]$ when $a = 1$, $b = 0$ and $\mathbb{Q}[i]$ is closed under addition and multiplication.

For subring $\mathbb{Q}[i]$, $1_R \neq 0_R$ so $\mathbb{Q}[i]$ is non-trivial. For non-zero element $\alpha \in \mathbb{Q}[i]$ let's say $\alpha = a+bi$ $a, b \in \mathbb{Q}$ If $\alpha \in \mathbb{Q}[i]$ is a unit, then $\alpha^{-1} \in \mathbb{Q}[i]$ such that $\alpha\alpha^{-1} = 1$ exists. Since $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$, Every non-zero element of $\mathbb{Q}[i]$ has a multiplicative inverse so. $\mathbb{Q}[i]$ is a field so $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$

Problem 3 (7.16)

Let D be an infinite integral domain, and let $g, h \in D[x]$. Show that if $g(x) = h(x)$ for all $x \in D$, then $g = h$. Thus, for an infinite integral domain D, there is a one-to-one correspondence between polynomials over D and polynomial function on D.

D is an integral domain so D is non-trivial and has no zero-divisors. we need to show if $g(x) = h(x)$ for all $x \in D$, then $g = h$. for two polynomials over D, g, h $g(x)$, $h(x)$ two function's values for all $x \in D$ are equal for infinite.

Using Theorem 7.12, since D, and $D[x]$ are integral domain (D is integral domain, so $D[x]$ is also integral domain) using the remainder property for polynomials, there exist unique $q, r \in D[x]$, such that $g(x) = (x-x)q + r$ with $q, r \in D[x]$ and $\deg(r) < 1$, which means $r \in R$ so if every element of D has the same output of $g(x) = h(x)$ then they are the same polynomials.

For each element D, there exists a unique polynomial for each element, so there is a one-to-one correspondence between polynomials over D and polynomial functions on D.

Problem 4 (7.20)

Let D be an integral domain, let $g, h \in D[x]$, and let $x \in D$. Show that $m_x(gh) = m_x(g) + m_x(h)$.

D is an integral domain. Integral domain is non-trivial and has no zero-divisor

g, h are polynomials of D[x]. D[x] is also an integral domain.

$M_x(g)$ denotes the value $0 \le m \le k$ and a polynomial $q \in R[x]$, such that

$$g = (X-x)^m q \text{ and } q(x) \neq 0$$

$g \in R[x]$.

$g = (X-x)^m q$ and $q(g) \neq 0$

$h = (x-x)^m q$ and $q(h) \neq 0$

Let's say $m_x(g) = k$ and $m_x(h) = l$. $g(y) \ldots = (X-x)^k q(g) \times (X-x)^l q(h)$

$\Rightarrow (x-m)^{k+l} \times q(y) \times q(h) \Rightarrow gh(y) = (X-x)^{k+l} q(h) q(g)$ so $m_x(gh) \ge k+l$

so $m_x(gh) \ge m_x(g) + m_x(h)$. If $m_x(gh) > m_x(g) + m_x(h)$ then x is a root $q(g) \cdot q(h)$

so $q(g) q(h) = 0$ then $q(g)$ or $q(h) = 0$ so x is a wt of $q(g)$ or $q(h)$

which is not true. so $m_x(gh) > m_x(y) + m_x(h)$ is not possible

Problem 5 (17.38)
Let R be a ring. An ideal I of R is called prime if $I \subsetneq R$ and if for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$. An ideal I of R is called maximal if $I \subsetneq R$ and there are no ideals J of R such that $I \subsetneq J \subsetneq R$ Show that:

(a) an ideal I of R is prime if and only if R/I is an integral domain.

Let's say ideal I of R is prime. Then for $a, b \in R$, ($a+b \in R$, $a \cdot b \in R$)
Then $(a+I) \times (b+I) = ab + aI + bI + I \cdot I$ which is also $\in I$. $a+I \in I$, $b+I \in I$
$a \in I$ and $b \in I$ so R/I is integral domain since it is non-trivial and has zero-divisor

Conversly. Let's say R/I is an integral domain which does not have zero divisor and non-trivial. Suppose $a+I$ and $b+I \in R/I$ so $(a+I) \times (b+I) = 0 \times I = I$
so $ab \in I$, $a \in I$ and $b \in I$ $a+I \in I$ and $b+I \in I$ so ideal I is prime

(b) an ideal I of R is maximal if and only if R/I is a field.

Let's say ideal I of R is maximal. Also say there is ideal $J \supsetneq I$ and element $t \in J$ but $t \notin I$ since $I \subsetneq I$ $t+I$ is a non-zero element of R/I since $t+I \notin I$
Let's say there is another element $v \in T$ $v+I \notin I$, $v+I \in R/I$
by additive and multiplication it has inverse so R/I is a field

Conversely R/I is a field, let $t \in R$ and $t \notin I$ need to show $b+I$ has multiplicative inverse. Let's say $J = \{t \cdot r + i \mid r \in R \text{ and } i \in I\}$ then J is ideal since additive closed and multiplication on I so ideal I of R is maximal

(c) all maximal ideals of R are also prime ideals

Since from theorem 7.6 Every field is integral domain. by part (a) and part (c) all maximal ideals of R are also prime ideals.

problem 6 (7.58)
Let $n = pq$, where p and q are distinct primes. Show that we have a ring isomorphism $\mathbb{Z}_n[x] \cong \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$

we have from the question $n = pq$ (distinct primes). By definition 7.20 ring homomorphism if $\phi(ab) = \phi(a)\,\phi(b)$ for all $a, b \in R$ And also by the polynomial evaluation map $\phi : R[x] \to E$ $\partial \mapsto \partial(\alpha)$ for fix α we have two disting p and q $\mathbb{Z}_p[x] \times \mathbb{Z}_p[x]$ is ring isomorphism to $\mathbb{Z}_n[x]$

problem 7 (7.59)

Let p be a prime with $p \equiv 1 \pmod 4$. Show that we have a ring isomorphism $\mathbb{Z}[x]/(x^2+1, p) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

From the question we know p is a odd prime $1+4z$ for $z \in \mathbb{Z}$ sot let I (x^2+1, p) using the condition that $p+I = 0+I$ so we can assume $\mathbb{Z}[x]/(x^2+1, p) = \{0+I, 1+I, x+I, x+1+I, x+2+I, 2x+I, \ldots\}$

$\mathbb{Z}[x]/(x^2+1, p)$ is the member of $\mathbb{Z}(1 \bmod 4)$

so in general $\frac{\mathbb{Z}[x]}{(x^2+1, p)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$