Date ___/___/_____

Keerti P. Charantimath MA exam
19MA20059

7) Aim : to find $17^2 . 7^2$ as a sum of two squares

We know that $17 \equiv 1 \pmod 4$ & $7 \equiv 3 \pmod 4$
Also, $17 = (1+4i)(1-4i) = (4+i)(4-i)$

number of ways that we can represent is
$4 \times (2+1) = 12$

Consider
$A+iB = 7(1+4i)(1+4i)$
(OR)
$7(1-4i)(1-4i)$
(OR)
$7(1+4i)(1-4i)$

Multiplying $A+iB$ with units in $Z[i]$
(we know that ± 1 and $\pm i$ are units in $Z[i]$)

Case 1:- taking unit as $(+1)$
$7(1+4i)(1+4i)$,
$7(1+4i)(1-4i)$,
$7(1-4i)(1-4i)$

Case 2:- taking unit as (-1)
$-7(1+4i)(1+4i)$,
$-7(1-4i)(1-4i)$,
$-7(1+4i)(1-4i)$

Case 3:- taking unis as $(+i)$
$7i(1+4i)(1+4i)$,
$7i(1-4i)(1-4i)$,
$7i(1+4i)(1-4i)$

Case 4:- taking unit as $(-i)$
$-7i(1+4i)(1+4i)$,
$-7i(1-4i)(1-4i)$,
$-7i(1+4i)(1-4i)$

Date ___ / ___ / ___

For each of the 12 cases we get
$17^2 \cdot 7^2 = A^2 + B^2$ form.

Saathi

Date ___ / ___ / _____

3) $Z(G) \rightarrow$ center of G
$G \rightarrow$ non-Abelian group } Given.

As $Z(G) \leq G$, we know that $|Z(G)|$ is a divisor of $|G|$. We can prove this using the Lagrange's theorem

G is of order 125 i.e $|G| = 125$.
This implies that $Z(G)$ can be of orders 1, 5, 25, 125

It is also given that $|Z(G)| \neq 1$.
It is also obvious that $|Z(G)|$ cannot be 125 as in that case $Z(G)$ would be same as G.
But G is not - an abelian group. Thus, $|Z(G)| \neq 125$.

We are left with orders 25 and 5.
Case 1 :- $|Z(G)| = 25$
This case is not possible as
$|G/Z(G)| = |G|/|Z(G)| = 5$
This leads to $Z/Z(G)$ being cyclic and thus implying that G is abelian which is not true

$\therefore$ case 1 is not possible

Case 2 :- $|Z(G)| = 25$ $\rightarrow$ this is the only possible case which does not lead to G being abelian or $Z(G)$ being non-abelian.

Hence, $|Z(G)| = 25$

Saathi

Date ___ /___ /______

1 b) We know

$f: F \to R$ is non-zero ring homomorphism and F is a field (Given)

Ker(f) is a ideal of F.

F has only two ideals (0) & (1)

ker(f) = (0) or (1)

Case 1 :- ker(f) = (1)

$1_s \in \ker(f) \Rightarrow f(1_s) = 0_R$ & $f(1_s) = 1_R$

$\Rightarrow 0_R = 1_R$

leads to a zero ~~ring~~ mapping

Not possible

Case 2 :- ker(f) = (0)

This is a possible case.

$\therefore \ker(f) = \{0\} \Rightarrow f$ is injective.

TRUE

1 c) Suppose R is the subring of field ~~F~~ F.

if $a \neq 0 \in R$ then $a^{-1} \in R$ as $a^{-1} \in F$ & $a.a^{-1} = 1 \in R$

we know that Ring is closed under multiplication

$\therefore a^{-1} \in R$

We know that Field is commutative ring which contains the multiplicative inverse of all elements exist

This is also true for R.

$\therefore$ R is a field.

TRUE

Date ___/___/___

1.e. $|G| = 23$

We know that any group of prime order is cyclic and 23 is a prime number.
We also know that every cyclic group is abelian.

Thus G is abelian group.
TRUE

1 a. For $Z \times Z$, the additive identity should be $(0,0)$
But we see that
$(a,0).(0,b) = (0,0)$ is true even when
$a \neq 0$ and $b \neq 0$

For $Z \times Z$ to be integral domain, $(0,0)$ should have no ~~zero~~ zero divisor.
But the above statement is not true in our case
Thus
$Z \times Z$ is non an integral domain

FALSE

1 d. Suppose R is an integral domain
Also suppose $R[x]/x \cong R$. $\rightarrow$ not a field
Thus, (x) is no maximal ideal.

We also know that R has no zero divisors.
Thus (x) is a prime ideal

FALSE

Date ___/___/______

6) $Z[\sqrt{-2}] \longrightarrow$ integral domain

We need to prove that $Z[\sqrt{-2}]$ has division algorithm

$N(x) = a^2 + 2b^2$ (here $x = a + b\sqrt{-2} \in Z[\sqrt{-2}]$)

Suppose $R = Z[\sqrt{-2}]$

We need to check that $\forall$ a, b $\in R$, and b non-zero, $\exists$ q, r st. $a = bq + r$ (where r is zero or $N(r) < N(b)$)

$x, y \in R$, $y \neq 0 \longrightarrow$ assume.

As $R(i)$ is subfield of $C \longrightarrow x \in R(i)$, $x \neq 0$ has multiplicative inverse

Let $z = xy^{-1} \in R(i)$, $x, y \in Z[\sqrt{-2}]$,

$w = c + d\sqrt{-2} \in Z[\sqrt{-2}]$

Suppose $z = a + b\sqrt{-2}$, $a, b \in R$ (here $|a-b| \leq \frac{1}{2}$ & $|b-d| \leq \frac{1}{2}$)

We see that, $z = w + (z-w)$

Page No. ______