PGMT Paper - 1A.

1) (a) Let G be a group in which, $(ab)^2 = a^2b^2$ for all $a, b \in G$. Show that $H = \{g^2 \mid g \in G\}$ is a normal subgroup of G.

⇒ Let $g \in G$ and $h \in H$ then $(gh)^2 \in H$ and $g^{-2} \in H$.

So, H is a subgroup of G. So $h^{-1}g^{-2} \in H$ and $(gh)^2 h^{-1}g^{-2} \in H$.

$\therefore ghghh^{-1}g^{-2} \in H$ i.e. $ghg^{-1} \in H$. Hence H is normal subgroup of G.

(b) Does there exist a non-commutative group G such that $|G/Z(G)|$ is a prime where $Z(G)$ denotes the centre of G? Jusify your answer.

⇒ Since we know that If G be a non-commutative group with centre Z then the quotient group G/Z is non-cyclic. Hence $|G/Z(G)|$ is not a prime. Hence there doesnot exist a such a group G.

(c) Prove that any epimorphism of the additive group $\mathbb{Z}$ onto the additive group $\mathbb{Z}$ is an isomorphism.

⇒ Since we know that two infinite cyclic groups are isomorphic. Since $(\mathbb{Z}, +)$ is a infinite cyclic grous. So any epimorphism of the additive group $\mathbb{Z}$ onto the additive group $\mathbb{Z}$ is an isomorphism.

(d) Let F be a Field, Prove that $\langle 0 \rangle$, the ideal consisting of zero element of F only, is a maximal ideal of F.

⇒ The ideal which only contains the zero element of F. is a maximal ideal of F since there is no proper ideal of F strictly containing the ideal $\{0\}$.

(e) Let F be a finite field of characteristic p. Prove that the mapping $f: F \to F^p$ defined by $f(x) = x^p$ for all $x \in F$ is an isomorphism where $F^p = \{a^p \mid a \in F\}$.

⇒ Let $x, y \in F$, then

$$f(x+y) = (x+y)^p = x^p + y^p$$
$$= f(x) + f(y)$$

Again $f(xy) = (xy)^p = x^p y^q = f(x) f(y)$

∴ f is homomorphism.

Also, $\ker f = \{0\}$. So f is ~~homomorphism~~ isomorphism

(f) Prove that in an integral domain D every prime element is irreducible

⇒ Let p be a prime element in an integral domain D.

Let $p = ab$, $a, b \in D$. Then $p \mid ab$ and since p is prime, either $p \mid a$ or $p \mid b$.

If $p \mid a$ then $a = pd_1$ for some d_1 in D. In this case $p = pd_1 b$.

$\Rightarrow$ $p(1-d_1 b) = 0$, 1 being the identity element in D.

$\Rightarrow$ $1 - d_1 b = 0$, since $p \neq 0$ and D contains no divisor of zero.

$\Rightarrow$ $d_1 b = 1$ and this shows that d_1 and b are units in D.

i.e a is an associate of p and b is a unit in D.

If $p|b$ then $b = pd_2$ for some d_2 in D. In this case $p = a p d_2$

and Similarly, a is a unit in D. and b is an associate of p.

$\therefore$ $p = ab$ implies either a is a unit and b is an associate of p, or b is a unit and a is an associate of p. Therefore p is an irreducible in D.

(8) Consider the field extension C/R where C is the field of complex numbers and R is the field of real no. Find a basis of C/R. Justify your answer.

$\Rightarrow$

h) Find the minimal polynomial of ω over $\mathbb{Q}$, the field of rational nos. where ω is a complex cube root of unity.

⇒ Let $a = \omega$.

Now, $a^3 - 1 = \omega^3 - 1 = 0$.

So a satisfies the polynomial $f(x) = x^3 - 1$ over $\mathbb{Q}$.

Also, the rational roots of f are ± 1.

Now, $f(1) = 0$, $f(-1) = -2$.

So $f(x)$ is irreducible over $\mathbb{Q}$.

∴ The minimal polynomial of ω over $\mathbb{Q}$ is

$$f(x) = x^3 - 1.$$

(a) Let G be a group of order p^2, where p is a prime. Prove that G is commutative.

⇒ Let Z be the centre of G. By Lagrange's theorem, $o(Z)$ is a divisor of p^2. Since p is a prime $\cdot o(Z) = 1$ or p or p^2. But $o(Z) \neq 1$. Since G, being a group of order p^2 has a non-trivial centre.

If possible, let $o(Z) = p$. Then the quotient group G/Z is of prime order p and is therefore cyclic. This is an impossibility, because for any group G the quotient-group G/Z cannot be non-trivial cyclic.

Hence $o(Z) = p^2$ and therefore $Z = G$. Consequently G is abelian.

(b) State Cauchy's theorem on groups. Use this theorem to prove that every group of order $2p$ where p is prime has a non-trivial normal subgroup.

⇒ Cauchy's theorem
Let G be a finite group. If p is a prime divisor of $o(G)$, then G has an element of order p.

By Cauchy's theorem, G has a subgroup H of order p. We show that the no. of subgroups of order p in G is only one.