SEMISTRAL ALGEBRA I SOLUTION 09.PDF

(1) Let G be any group of order p^2, p prime. For $g \in G$, let $N(g)$ denotes its normalizer in G. Then by the class formula for G, we have $|G|$ is $|Z(G)| + \sum_{N(a)\neq G} \frac{|G|}{|N(a)|}$. Now $a \in Z(G)$ if and only if $N(a)$ is same as G. As G has order p^2 and for $a \notin Z(G)$, $|N(a)| < |G|$, $p \| Z(G)|$. So $Z(G) \neq \{e\}$. Assume that $|Z(G)|$ is p. Let $g \in G$, $g \notin Z(G)$. So $N(g)$ is a subgroup of G strictly containing $Z(G)$ (since $g \in N(g) \setminus Z(G)$). Hence $|N(g)| > p$. But by Lagrange's Theorem, $|N(g)|$ divides p^2. So $g \in Z(G)$, a contradiction. Thus $Z(G)$ must have order p^2, and so G is abelian.

(2) H is the unique normal p-Sylow subgroup of $N(H)$. If $x \in N(N(H))$ then $xN(H)x^{-1} = N(H)$ so $xHx^{-1} \subseteq xN(H)x^{-1} = N(H)$. As conjugate of a p-Sylow subgroup is again a p-Sylow subgroup, we have $xHx^{-1} = H$, so $x \in N(H)$. Thus $N(N(H)) \subseteq N(H)$. But $N(H) \subseteq N(N(H))$. Hence $N(N(H)) = N(H)$.

(3) We have an isomorphism $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$. Via this isomorphism i corresponds to $\hat{X}$ (the residue class of X), and therefore the ideal $(2+i)$ corresponds to $(2+\hat{X}) = (2+X, X^2+1)/(X^2+1)$. Now

$$\frac{\mathbb{Z}[X]/(X^2+1)}{(2+X, X^2+1)/(X^2+1)} \cong \frac{\mathbb{Z}[X]}{(2+X, X^2+1)} \cong \frac{\mathbb{Z}[X]/(2+X)}{(2+X, X^2+1)/(2+X)}.$$

But $\mathbb{Z}[X]/(2+X) \cong \mathbb{Z}$, by sending X to -2, so

$$\frac{\mathbb{Z}[X]/(2+X)}{(2+X, X^2+1)/(2+X)} \cong \mathbb{Z}/((-2)^2+1) = \mathbb{Z}/(5).$$

Thus $\frac{\mathbb{Z}[i]}{(2+i)}$ is the finite field $\mathbb{F}_5$.

(4) For any $n \in \mathbb{N}$, the ideals of $\mathbb{Z}/(n)$ are (d), ideals generated by d, such that $d|n$. For ideals (d_1), (d_2) of $\mathbb{Z}/(n)$, $(d_1) \subseteq (d_2)$ if and only if $d_2|d_1$. Now $n = 32 = 2^5$. So the prime ideals are of the form (2^i) for $1 \leq i \leq 5$. but for $i \geq 2$, neither 2 or 2^{i-1} are in (2^i), but their product is. So the only prime ideal of $\mathbb{Z}/(32)$ is the ideal (2), which is also maximal. So the nilradical is same as the Jacobson radical, equal to the ideal (2).

(5) $12 = 2^2 \times 3$. So the ideals of $\mathbb{Z}/(12)$ are $\{0\}$, (2), (3), (4) and (1). For $n \in \mathbb{N}$, $d|n$, $(\mathbb{Z}/(n))/(d) \cong (\mathbb{Z}/(d))/(n) \cong \mathbb{Z}/(d)$. So the respective quotients are isomorphic to $\mathbb{Z}/(12)$, $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(4)$ and $\{0\}$.

(6) $X^2 - X + 6 = X^2 - X - 6 = (X-3)(X+2)$ in $\mathbb{Z}/(12)$. So 3 and 10 are solutions of the equation modulo 12. The polynomial has two other zeros, namely 6 and 7.

(7) **Claim:** There is a one-to-one correspondence between {Ideals of R containing I} and {Ideals of R/I}.

For an ideal J of R containing I, J/I is an ideal of R/I. Conversely, let $\tilde{J}$ be any ideal of R/I, $\pi : R \to R/I$ the canonical surjection, J be the preimage of $\tilde{J}$ under π. For $r \in R$, $j \in J$, $\pi(r \cdot j) = \pi(r) \cdot \pi(j) \in \tilde{J}$. So $r \cdot j \in J$, showing that J is an ideal of R. As $\pi(I) \subset \tilde{J}$ in R/I, $I \subset J$. This proves the claim.