Exercise5.5

Proof. If π is an associate of an integer prime, i.e. $\pi = u \cdot p$, p is a integer prime. Then $\overline{\pi} = \overline{u} \cdot \overline{p} = \overline{u} \cdot p$ is associated with π. $(*)$

If π is not an associate of an integer prime.

Then for $\pi = a + bi, a, b \neq 0, a, b \in \mathbb{Z}$, $\pi, \overline{\pi}$ are associated if and only if $a + bi = u \cdot (a - bi)$, where u is a unit, i.e. $u \in \{1, -1, i, -i\} \Leftrightarrow (a + bi) = u \cdot (a - bi)$ for $u \in \{i, -i\}$. $\Leftrightarrow (a, b) = (b, a)$ or $(a, b) = (-b, -a)$. $\Leftrightarrow a^2 = b^2$.

Now, assume $a^2 = b^2$, by Theorem 12.5.2(a), $\pi \cdot \overline{\pi} = a^2 + b^2 = 2a^2$ is an integer prime or the square of an integer. $2|2a^2 \Rightarrow 2a^2 = 2or4 \Rightarrow 2a^2 = 2$ $(a \in \mathbb{Z})$ So $\pi \cdot \overline{\pi} = 2$.

If $\pi \cdot \overline{\pi} = 2$, i.e. $a^2 + b^2 = 2$. Since π is not an associate of an integer prime, then $a, b \geq 1$, $\Rightarrow a^2 = b^2 = 1$ $\Rightarrow \pi = 1 + i$ or $\pi = 1 - i \Rightarrow \pi, \overline{\pi}$ are associated.

So we have proved that if π is not an associate of an integer prime, then π and $\overline{\pi}$ are associates if and only if $\pi\overline{\pi} = 2$. It implies the original problem by $(*)$. □

Exercise5.6

Proof. Since

$$
\begin{aligned}
\mathbb{Z}[\sqrt{-3}]/(p) &\cong \mathbb{Z}[x]/(x^2+3)/(p) && (1)\\
&\cong \mathbb{Z}[x]/(p, x^2+p) && (2)\\
&\cong \mathbb{Z}[x]/(p)/(x^2+3) && (3)\\
&= \mathbb{F}_p[x]/(x^2+3) && (4)
\end{aligned}
$$

p is prime in $\mathbb{Z}[\sqrt{-3}] \Leftrightarrow \mathbb{Z}[\sqrt{-3}]/(p)$ is integral domain $Leftrightarrow$ $\mathbb{F}_p[x]/(x^2+3)$ is integral domain $\Leftrightarrow x^2 + 3$ is prime in $\mathbb{F}_p[x] \Leftrightarrow x^2 + 3$ is irreducible in $\mathbb{F}_p[x]$ since $\mathbb{F}_p[x]$ is PID. □

3. Let $R := \{\sum\limits_{i=0}^{n} a_i t^i \in \mathbb{C}[t] : a_1 = 0\}$, which is a subring in $\mathbb{C}[t]$

For $f(t) = \sum\limits_{i=0}^{n} a_i t^i \in R, a_1 = 0$, we have

$$\varphi(a_0 + \sum_{3 \leq i \leq n, 2|i} a_i x^{\frac{i}{2}} + \sum_{3 \leq i \leq n, 2|(i-1)} a_i x^{\frac{i-3}{2}} y) = f(t)$$

Moreover, for $x^a y^b \in \mathbb{C}[x, y]$, we have $\varphi(x^a y^b) = t^{2a+3b}$ of degree ≥ 2 if $x^a y^b$ is not a constant. So $\varphi(f) \in R$.

Therefore, φ can induce $\hat{\varphi} : \mathbb{C}[x, y]/\ker\varphi \to R$ bijection, moreover, an isomorphism since R is a subring in $\mathbb{C}[t]$.

So it suffices to prove the induced map $\mathrm{Spec}(\mathbb{C}[t]) \to \mathrm{Spec}(R), p \mapsto p \cap R$ is bijective.

Since $\mathbb{C}[t]$ is PID, prime ideal in $\mathbb{C}[t]$ are exactly (p), where $p = x + c, c \in \mathbb{C}$ prime element in $\mathbb{C}[t]$.

Then for $(x+c_1), (x+c_2)$ prime ideal in $\mathbb{C}[t]$, $c_1 \neq c_2$, $x^3 + c_1 x^2 \in (x+c_1) \cap R$. But if $x^3 + c_1 x^2 \in (x+c_2)$, then $x^2 \in (x+c_2)$ since $x + c_1 \notin (x+c_2)$. So $c_2 = 0$. But now $x^2 \notin (x+c_1) \Rightarrow (x+c_1) \cap R \neq (x+c_2) \cap R$. Otherwise, if $x^3 + c_1 x^2 \notin (x + c_2)$, then $(x + c_1) \cap R \neq (x + c_2) \cap R$. Therefore, the induced map should be injective.

Define $\mathbb{C}[t^n] = \{\sum_{i=0}^{n} a_i t^{in} : a_i \in \mathbb{C}\}$ be a subring of R if $n \geq 2$, moreover, a PID since it is equivalent to replace t with t^n in $\mathbb{C}[t]$.

For P prime ideal in R. For $n \geq 2$, the inclusion homomorphism $\mathbb{C}[t^n] \to R$ induce the map $\mathrm{Spec}R \to \mathrm{Spec}\mathbb{C}[t^n]$. Then $P \cap \mathbb{C}[t^n]$ is a prime ideal in $\mathbb{C}[t^n]$. So $P \cap \mathbb{C}[t^2] = (t^2 + c)\mathbb{C}[t^2], P \cap \mathbb{C}[t^3] = (t^3 + c')\mathbb{C}[t^3]$. Let $c = -k^2$ for some $k \in \mathbb{C}$. Since $(t^3 + k^3)(t^3 - k^3) = t^6 - k^6 \in (t^2 - k^2)\mathbb{C}[t^2] \subset P$, $\Rightarrow t^3 + k^3 \in p$ or $t^3 - k^3 \in P$. Then we have $t^3 + k^3 \in P \cap \mathbb{C}[t^3] = (t^3 + c')\mathbb{C}[t^3]$ or $t^3 - k^3 \in P \cap \mathbb{C}[t^3] = (t^3 + c')\mathbb{C}[t^3]$, which means $P \cap \mathbb{C}[t^3] = (t^3 + k^3)\mathbb{C}[t^3]$ or $(t^3 - k^3)\mathbb{C}[t^3]$.

WLOG, we assume that $P \cap \mathbb{C}[t^3] = (t^3 + k^3)\mathbb{C}[t^3]$(otherewise we replace k with -k). For $f = \sum_{i=0}^{n} a_i t^i \in R$, $f = g(t^2 - k^2) + rt + s$ where $g \in \mathbb{C}[t], r, s \in \mathbb{C}[t]$. Let $g = g' + mt, g' \in R$. Then

$$f = g'(t^2 - k^2) + mt^3 - mk^2 t + rt + s$$

$g'(t^2 - k^2) \in P$. Since $f \in R$, $(r - mk^2)t = 0$. So $f \in P$ if and only if $mt^3 + s \in P \Leftrightarrow mt^3 + s \in (t^3 + k^3)\mathbb{C}[t^3]$ $\Leftrightarrow s = mk^3 \Leftrightarrow f(-k) = g'(-k)((-k)^2 - k^2) + m(-k)^3 + s = 0 \Leftrightarrow (x + k)|f$. So $P = (x + k) \cap R$

Therefore every prime ideal P in R should be the intersection of prime ideal in $\mathbb{C}[t]$ and R. Which means the induced map is surjective.

So the induced map is bijective.

For group G of order 2275

4. Let n_p denote the number of Sylow p-subgroup. By Third Sylow Theorem, we have

$n_7 \equiv 1 \pmod 7$, $n_7 \mid 5^2 \cdot 13 \Rightarrow n_7 = 1$

$n_{13} \equiv 1 \pmod{13}$ $n_{13} \mid 5^2 \cdot 7 \Rightarrow n_{13} = 1$.

Let K_7, K_{13} be the unique Sylow 7-subgroup, 13-subgroup respectively.

Then $K_7 \lhd G$, $K_{13} \lhd G$ by second Sylow thm.

Since $K_7 \cap K_{13} < K_7, K_{13} \Rightarrow |K_7 \cap K_{13}| \mid |K_7|, |K_{13}|$

$\Rightarrow K_7 \cap K_{13} = \{1\}$

Then by Prop 7.3.3, $K_7 K_{13} \cong K_7 \times K_{13}$.

Since K_7, K_{13} cyclic, hence abelian, $K_7K_{13} \cong K_7 \times K_{13}$ is abelian.

$\forall g \in G$, $g K_7 K_{13} g^{-1} = g K_7 g^{-1} g K_{13} g^{-1} = K_7 K_{13} \Rightarrow K_7 K_{13} \lhd G$

Let K_5 be the Sylow 5-subgroup.

Choose $g \neq 1$ in K_5.

Let $H = \langle g \rangle$

Let $S \subset K_7 K_{13}$ denote all elements of order 91.

For $h \in H$, $s \in S$, $hsh^{-1} \in K_7 K_{13}$ since $K_7 K_{13} \lhd G$.

$(hsh^{-1})^n = hs^nh^{-1} = 1$ if and only if $s^n = 1 \Rightarrow hsh^{-1} \in S$ has order of 91

Consider action $H \curvearrowright S$, $h * k = hkh^{-1} \in S$

Since $K_7 K_{13} \cong K_7 \times K_{13}$, $|S| = |\{(e_1, e_2) \in K_7 \times K_{13} : e_1 \neq 1 \text{ or } e_2 \neq 1\}|$

$= 6 \times 12 = 72$.

order of orbit in S should divide $|H| \mid 25$

$|S| = 72$

$\Rightarrow$ $\exists$ orbit of order 1. i.e. $\exists k \in S$, $gkg^{-1} = k$.

$\Rightarrow k^n = (g k g^{-1})^n = g k^n g^{-1}$

since k has order of 91 $\Rightarrow$ g commutes with all elements in $K_7 K_{13}$

Thus $\forall g \in K_5$, g commutes with all elements in $K_7 K_{13}$

By 2^{nd} isom thm $K_5(K_7K_{13}) < G$, $|K_5(K_7K_{13})| = \dfrac{|K_5||K_7K_{13}|}{|K_5 \cap K_7K_{13}|} = 2275 = |G|$

$\Rightarrow K_5(K_7K_{13}) = G$

$\forall h_1, h_2 \in K_5$, $k_1, k_2 \in K_7K_{13}$

$$h_1k_1h_2k_2 = h_1h_2k_1k_2 = h_2h_1k_2k_1 \quad (K_5 \text{ has order of } 5^2\text{, hence abelian})$$
$$= h_2k_2h_1k_1$$

$\Rightarrow G = K_5(K_7K_{13})$ commutes