Problem 1.

Show the polynomial

\[ f(x) = x^4 - 5(1 - i)x + 5 \]

is irreducible in \( \mathbb{Z}[i][x] \).

Consider the prime

\[ p = 1 + 2i \]

in \( \mathbb{Z}[i] \). This is prime because the norm \( N(p) = 5 \) is a prime integer. Clearly,

\[ 5 = p \cdot \overline{p} \]

is not divisible by \( p^2 \) since \( \overline{p} = 1 - 2i \) is not divisible by \( p \) (they have equal norms, hence they will have to differ by a unit \( \pm 1, \pm i \) which they don’t). We apply the Eisenstein criterion for the prime \( p \) to conclude.
Problem 2.

Let $A$ be a Dedekind domain, and $a, b, c$ be three ideals in $A$. Prove that

$$a \cap (b + c) = a \cap b + a \cap c.$$

(i) First prove this assertion when $A$ is a DVR.

Assume that $A$ is a DVR. Then pick a uniformizer $x$ and write

$$b = (x^b), \quad c = (x^c).$$

Assume $b \geq c$. Then

$$b \subset c \implies a \cap b \subset a \cap c.$$

The identity is trivially satisfied since

$$b + c = c, \quad a \cap b + a \cap c = a \cap c.$$

(ii) Localize to obtain the statement for any Dedekind domain.

For any prime $p$ in $A$, $A_p$ is a DVR. Localize at $p$ and use (i). We have

$$(a \cap (b + c))_p = a_p \cap (b + c)_p = a_p \cap (b_p + c_p)$$

$$= a_p \cap b_p + a_p \cap c_p$$

$$= (a \cap b)_p + (a \cap c)_p$$

$$= (a \cap b + a \cap c)_p.$$

Using that for any ideal $i$ we have

$$i = \cap i_p,$$

for

$$i = a \cap (b + c), \quad \text{and} \quad i = a \cap b + a \cap c$$

respectively, we are done.
Problem 3

Consider $p \equiv 1 \mod 3$ a prime number.

(i) Prove that there exists $x \in \mathbb{F}_p^* \setminus \{1\}$ such that $x^3 \equiv 1 \mod p$.

Consider $g$ a generator for the cyclic group $\mathbb{F}_p^*$ and set $x = g^{p-1}$. Clearly,

$$x^3 = g^{3(p-1)} = 1, \quad x \neq 1.$$ 

(ii) Using (i), prove that $p$ is not a prime in the ring $\mathcal{O}$ of quadratic integers of $\mathbb{Q}(\sqrt{-3})$.

**Assume $p$ is prime.** Let $\omega = \frac{-1 + \sqrt{-3}}{2}$. Then

$$p|x^3 - 1 = (x - 1)(x - \omega)(x - \bar{\omega}) \Rightarrow p|1 \text{ or } p|x - \omega \text{ or } p|x - \bar{\omega}.$$ 

But this is impossible. The first case implies

$$x - 1 = p\alpha, \quad \alpha \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z} \Rightarrow x = 1 \text{ in } \mathbb{F}_p,$$

while the last two cases are impossible by looking at the coefficient of $\omega$. We conclude $p$ is not prime.

(iii) Considering the prime factorization of $p$ in $\mathcal{O}$, show that there are integers $a$ and $b$ such that

$$p = a^2 + ab + b^2.$$ 

Write

$$p = \pi_1 \ldots \pi_k,$$

as product of primes in $\mathcal{O}$. Then taking norms, we find

$$p^2 = N(\pi_1) \ldots N(\pi_k).$$

We must have $N(\pi_1) = p$. Write $\pi_1 = a + b\omega$ with norm $a^2 - ab + b^2 = a^2 + a(-b) + (-b)^2$, completing the proof.
Problem 4.

Which of the following rings are isomorphic?

(i) \( \mathbb{C}[t] \)
(ii) \( \mathbb{C}[x, y]/(x^2 + y^2) \)
(iii) \( \mathbb{C}[x, y]/(y^2 - x^5) \)
(iv) \( \mathbb{C}[x, y, z]/(y - x^3, z - x^5) \)

We claim that (i) and (iv) are isomorphic, while (i), (ii) and (iii) are not.

- We check (i) and (iv) are isomorphic. Define
  \[ f : \mathbb{C}[t] \to \mathbb{C}[x, y, z]/(y - x^3, z - x^5), \quad t \to (t, t^3, t^5), \]
  and
  \[ f : \mathbb{C}[x, y, z]/(y - x^3, z - x^5) \to \mathbb{C}[t], \quad (x, y, z) \to x. \]
  Clearly \( f \) and \( g \) are inverse morphisms.

- We show (ii) cannot be isomorphic to (i) and (iv). This follows observing that (i) and (iv) are integral domains, while (ii) is not. Indeed, for (ii), the polynomial \( x^2 + y^2 \) is reducible as \( x^2 + y^2 = (x + iy)(x - iy) \) so the quotient (ii) has zero divisors \( x \pm iy \).

  To show (iv) is an integral domain, it suffices to prove that the polynomial \( x^2 - y^5 \) is irreducible. Assuming the contrary, write
  \[ x^2 - y^5 = f_1(x, y) f_2(x, y). \]
  Regarding \( f_1, f_2 \) as polynomials in \( x \) with coefficients in the integral domain \( k[y] \), we conclude that \( f_1, f_2 \) can have degree at most 2 with respect to \( x \). In fact, it is clear that the combination of degrees \((0, 2)\) cannot occur. If the degrees are 1, we may assume
  \[ f_1(x, y) = x - g(y), f_2(x, y) = x - h(y). \]
  Then
  \[ x^2 - y^5 = x^2 - x (g(y) + h(y)) + g(y)h(y). \]
  Therefore,
  \[ g(y) = -h(y), \quad \text{and} \quad y^5 = g(y)h(y) = -g(y)^2. \]
  This is clearly impossible, proving our claim.

- We show that (i) and (iii) are not isomorphic. Assume there is an isomorphism
  \[ \Phi : \mathbb{C}[x, y]/(x^2 - y^5) \to \mathbb{C}[t]. \]
  Indeed, set
  \[ \Phi(x) = p, \Phi(y) = q. \]
We must have
\[ p^2 = q^5. \]
This implies that all irreducible factors appearing in \( q \) have even exponent, so
\[ q = r^2, \quad p = r^5 \]
for some polynomial \( r \). Note that \( r \) cannot be constant since otherwise the image of \( \Phi \) would have to consist in constant polynomials.

Now since \( \Phi \) is surjective, there is a polynomial
\[ f = \sum_{i,j} a_{i,j} x^i y^j \]
such that \( \Phi(f) = r \). This means that
\[ \sum_{i,j} a_{i,j} r^{5i+2j} = r. \]
In particular, since the left hand side must be divisible by \( r \), we have \( a_{00} = 0 \). However, since \( 5i + 2j \geq 2 \) for \((i, j) \neq (0, 0)\), the left hand side is in fact divisible by \( r^2 \), so it cannot equal \( r \). This contradiction shows that an isomorphism \( \Phi \) cannot exist.
Problem 5.

(i) Show that if $f, g \in \mathbb{C}[x, y]$ are distinct irreducible polynomials, then there exists $h \in \mathbb{C}[x]$ and polynomials $A, B \in \mathbb{C}[x, y]$ such that

$$h = fA + gB.$$ 

(ii) Using (i), show that the prime ideals $p$ in the polynomial ring $\mathbb{C}[x, y]$ are:

- the zero ideal $(0)$;
- the principal ideals $(f)$ where $f \in \mathbb{C}[x, y]$ is irreducible;
- the maximal ideals of the form $(x - a, y - b)$ for $(a, b) \in \mathbb{C}^2$.

(iii) Conclude that the Krull dimension of $\mathbb{C}[x, y]$ is 2.

(i) Consider $f, g$ as polynomials in $K[y]$ where $K = \mathbb{C}(x)$ is the fraction field of $R = \mathbb{C}[x]$. Note that $f, g$ are irreducible in $R[y]$, hence also in $K[y]$ by Gauss’ lemma. Thus $f$ and $g$ are coprime, hence we can find $\tilde{A}, \tilde{B} \in K[y]$ with

$$f \tilde{A} + g \tilde{B} = 1.$$

Writing the coefficients of $\tilde{A}$ and $\tilde{B}$ with a common denominator $h(x)$ and multiplying the above equality by $h$ we obtain the claim for

$$A = h\tilde{A}, B = \tilde{B}.$$

(ii) Assume $p \neq 0$. If $p$ is principal, generated by $f \in \mathbb{C}[x, y]$, then $f$ must be irreducible.

Otherwise, assume $p$ contains two distinct elements $f, g$ which are not multiples of each other. We may assume $f$ and $g$ are irreducible since otherwise we may replace them by some of their irreducible factors which must be in $p$ since $p$ is prime.

Now, by (i), we can find $h \in \mathbb{C}[x]$ such that

$$h = fA + gB$$

for some polynomials $A, B \in \mathbb{C}[x, y]$. Note that $h \in p$. Factor $h$ into linear factors. One of the linear factors $x - a$ must be in $p$. Similarly, we show $y - b \in p$ for some $b \in \mathbb{C}$. Therefore, the maximal ideal

$$(x - a, y - b) \subset p \implies p = (x - a, y - b),$$

completing the proof.

(iii) Clearly, a chain of length 2 is given by

$$(0) \subset (x + y) \subset (x, y).$$

If we have a chain of length 3

$$p_0 \subset p_1 \subset p_2 \subset p_3$$

then $p_1$ and $p_2$ cannot be zero or maximal, hence they must be generated by elements $(f)$ and $(g)$, for $f$ and $g$ irreducible. But since $p_1 \subset p_2$ we must have $g|f$ which is impossible.
Problem 6.

(i) Let $G$ be a finite group acting on a set $S$. Show that the number of orbits equals

$$\frac{1}{|G|} \sum_{g \in G} |S^g|$$

where $S^g$ is the fixed set of $g \in G$.

We consider the set

$$A = \{(g, s) : gs = s\}$$

and count its elements in two ways. First, $A$ is the union

$$\bigcup_{g \in G} \{g\} \times S^g$$

so it must have

$$|A| = \sum_{g} |S^g|$$

elements. Secondly, $A$ is union

$$\bigcup_{s \in S} \text{Stab}_G(s) \times \{s\}$$

which has

$$|A| = \sum_{s} |\text{Stab}_G(s)| = \sum_{s} \frac{|G|}{|O_s|}$$

where $O_s$ is the orbit of $s$. In turn

$$\sum_{s} \frac{1}{|O_s|} = \text{number of orbits},$$

since each orbit $O$ contributes $1 = \frac{1}{|O|} \cdot |O|$ for each of its elements. This gives

$$\sum_{g} |S^g| = |G| \cdot \text{number of orbits}.$$ 

(ii) How many distinct colorings of the regular hexagon with 3 colors are there? Two colorings are considered equivalent if they differ by a rigid symmetry.

The rigid symmetries of the hexagon is $D_6$. There are 12 elements in this group: the identity, 5 rotations $1, r, r^2, r^3, r^4, r^5$ and the symmetries along the 3 diagonals and the 3 lines joining the midpoints. We enumerate the fixed sets of each group element:

1. The identity has $n^6$ options.
2. The rotations $r, r^5$ has $n$ options since vertices have to be of the same color.
3. Rotations $r^2, r^4$ have a fixed set with $n^2$ elements since the every other vertex has to have the same color.
4. Rotation $r^3$ has $n^3$ fixed colorings since opposite vertices have the same color.
(5) Each symmetry along the diagonal has $n^4$ fixed colorings.

(6) Each symmetry along the lines joining midpoints has $n^3$ fixed colorings.

We find

$$\frac{1}{12}(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)$$

which is 92 colorings for $n = 3$. 
Problem 7.

Consider a group $G$ with 63 elements.

(i) Show that $G$ is solvable.

We look at the Sylow subgroups

$$n_7|3, n_7 \equiv 1 \mod 7 \implies n_7 = 1.$$ 

Consider $H$ a Sylow 7-subgroup. Then $H$ is normal in $G$. Clearly

$$H \cong \mathbb{Z}/7\mathbb{Z}$$

so $H$ is solvable. The quotient $G/H$ has 9 elements hence it is abelian, hence solvable. It follows that $G$ is solvable as well.

(ii) Describe all groups $G$ up to isomorphism.

There are 5 isomorphism classes. Consider a 3-Sylow $K$ which has 9 elements. Clearly,

$$|G| = |H||K|, \ H \cap K = \{1\}, \ H \normal $$

Therefore, these three statements imply

$$G = H \times_\phi K$$

for some

$$\phi : K \rightarrow Aut(H).$$

We have

$$Aut(H) = \mathbb{Z}/6\mathbb{Z}.$$ 

**Case 1.** If $K \cong \mathbb{Z}/9\mathbb{Z}$, letting $k$ be the generator of $K$, then $\phi(k)$ is an automorphism of $H$ of order dividing $6 = |Aut(H)|$ and $9 = |K|$ at the same time, hence either trivial or of order 3. The trivial automorphism gives the group

$$G = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$ 

There are two automorphisms of $H$ of order 3. One of them is

$$\psi(h) = h^2$$

where $h$ is a generator of $H$. The other one is

$$\tilde{\psi} = \psi^{-1} : h \rightarrow h^4$$

which can be described as

$$\tilde{\psi} = \psi \circ i$$

where

$$i(h) = h^2$$

is an automorphism of $H$. 

If the order of $\phi(k)$ is 3 then $\phi(k)$ is either $\psi$ or $\psi^{-1}$. Both cases give isomorphic groups

$$G = \langle h, k : h^9 = 1, k^7 = 1, hkh^{-1} = k^2 \rangle.$$ 

**Case 2.** If $K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, say generated by $x$ and $y$, we must have $\phi(x)$ of order 1 or 3, $\phi(y)$ of order 1 or 3.

(i) If $\phi(x)$ and $\phi(y)$ are trivial, we obtain

$$G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$ 

(ii) If $\phi(x)$ and $\phi(y)$ are of order 3, they can both be $\psi$ or $\tilde{\psi}$ in which case we obtain isomorphic groups

$$G = \langle h, x, y : h^7 = 1, x^3 = y^3 = 1, xy = yx, xhx^{-1} = h^2, yhy^{-1} = h^2 \rangle.$$ 

If one of them is $\psi$, the other is $\tilde{\psi}$ we may replace the generator $y$ by $y^2$ to place ourselves in the above situation.

(iii) If $\phi(x) = 1$ and $\phi(y)$ has order 3, or the other way around, we obtain

$$G = \mathbb{Z}/3\mathbb{Z} \times G'$$ 

where

$$G' = \langle h, y : h^7 = y^3, yhy^{-1} = h^2 \rangle.$$
Problem 8.

Let $G$ be an abelian subgroup of the symmetric group $S_{300}$. Show that $G$ has at most $3^{100}$ elements.

(i) Let $n \geq 1$ and assume $A$ is an abelian subgroup of $S_n$ which acts transitively on the set \{1, 2, \ldots, n\}. Show that the stabilizer of 1 is trivial, and conclude that $A$ must have $n$ elements.

(ii) Let $O_1, \ldots, O_s$ be the orbits of $G$ on the set \{1, 2, \ldots, 300\}. Fix such an orbit $O_i$, and note that each $g \in G$ permutes the elements of the orbit $O_i$. Write $A_i$ for the group of permutations of $O_i$ which come from elements $g \in G$. Use (i) to explain that $|A_i| = |O_i|$.

(iii) Show that $G$ is a subgroup of $A_1 \times \ldots \times A_s$.

(iv) Let $m_1, \ldots, m_s$ be the number of elements of the orbits $O_1, \ldots, O_s$. Using (ii) and (iii), conclude that $|G| \leq m_1 \ldots m_s$ where $m_1 + \ldots + m_s = 300$.

(v) Using (iv), and possibly a bit of calculus, prove that $|G| \leq 3^{100}$.

(vi) Give an example of an abelian subgroup of $G$ with $3^{100}$ elements.

(i) If $\sigma \in A$ has the property that $\sigma(1) = 1$, we show $\sigma = 1$. It suffices to prove that if $1 \leq j \leq n$ then $\sigma(j) = j$.

Indeed, let $\tau \in A$ such that $\tau(1) = j$, which exists since the action is transitive. Since $A$ is abelian,

$$\sigma \tau = \tau \sigma \implies \sigma(\tau(1)) = \tau(\sigma(1)) \implies \sigma(j) = j.$$  

As the stabilizer of 1 has one element, $A$ must have $n$ elements.

(ii) Note that $A_i$ acts on $O_i$ transitively by definition. Also $A_i$ is abelian, being a subgroup of $G$. Then by (i),

$$|A_i| = |O_i|.$$  

(iii) Each $g \in G$ gives an element $\sigma_i$ of $A_i$ so we obtain a group homomorphism

$$G \to A_1 \times \ldots \times A_s, g \mapsto (\sigma_1, \ldots, \sigma_s).$$  

We show this is injective by proving the kernel is trivial. If $\sigma_1 = 1, \ldots, \sigma_s = 1$, it means that $g$ keeps each element of $O_1$ fixed, and similarly for $O_2, \ldots, O_s$. Thus $g$ does not permute the set \{1, 2, \ldots, 300\} or said it differently, $g$ is the trivial permutation.

(iv) There is really nothing to prove here:

$$|G| \leq |A_1 \times \ldots \times A_s| = |A_1| \ldots |A_s| = m_1 \ldots m_s.$$  

(v) Let $a$ be the number of orbits with 1 element, $b$ the number of orbits with 2 elements, and $n_1, \ldots, n_r \geq 3$
be the number of elements in the orbits with at least 3 elements. Then
\[ a + 2b + n_1 + \ldots + n_r = 300. \]

Then,
\[ 2b + 3r \leq 300 \implies r \leq \frac{300 - 2b}{3}. \]

We have
\[ |G| \leq m_1 \ldots m_s = 2^b n_1 \ldots n_r \leq 2^b \left( \frac{n_1 + \ldots + n_r}{r} \right)^r \leq 2^b \left( \frac{300 - 2b}{r} \right)^r. \]

We keep \( b \) fixed, and consider the function
\[ f(r) = \left( \frac{300 - 2b}{r} \right)^r \text{ and } F(r) = \ln f(r) = r \ln \frac{300 - 2b}{r}, \]

We maximize \( f \) and \( F \). Note that
\[ F'(r) = \ln \frac{300 - 2b}{r} - 1 \geq \ln 3 - 1 > 0. \]

Thus \( F \) and \( f \) are increasing, hence the maximum of \( f \) occurs for
\[ r = \frac{300 - 2b}{3}. \]

Thus, we have
\[ |G| \leq 2^b 3^{\frac{300-2b}{3}} = 3^{100} \left( \frac{2}{3^{2/3}} \right)^b \leq 3^{100}. \]

(vi) Let \( \sigma_1 \) be the cycle \((123)\), \( \sigma_2 \) be the cycle \((456)\), etc \( \sigma_{100} \) be the cycle \((298\ 299\ 300)\). These cycles commute, and each generates a subgroup with 3 elements. These 100 subgroups are distinct. Their internal product in \( S_{300} \) is an abelian subgroup of \( S_{300} \) isomorphic to
\[ \mathbb{Z}/3\mathbb{Z} \times \ldots \mathbb{Z}/3\mathbb{Z}, \]

which has \( 3^{100} \) elements.
Problem 9.

Let $k \geq 1$. Consider $A$ the ring of polynomials $f \in \mathbb{C}[x]$ such that

$$f'(0) = f''(0) = \ldots = f^{(k)}(0) = 0.$$ 

Is $A$ Noetherian?

The elements of $A$ are of the form

$$f = a + x^{k+1}F(x).$$

Let $a$ be an ideal in $A$ which is not finitely generated. Successively pick elements

- $f_1 \in a$ of smallest possible degree $f_1 = a_1 + x^{k+1}F_1$,
- $f_2 \in a \setminus \langle f_1 \rangle$, of smallest possible degree $f_2 = a_2 + x^{k+1}F_2$,
- $f_\ell \in a \setminus \langle f_1, \ldots, f_{\ell-1} \rangle$ of smallest possible degree, $f_\ell = a_\ell + x^{k+1}F_\ell$

Write $d_1, \ldots, d_\ell, \ldots$ for the degrees of the $F_i$’s such that

$$d_1 \leq d_2 \leq \ldots d_\ell \leq \ldots$$

Multiplying by suitable constants we may assume $F_1, F_2, \ldots, F_\ell \ldots$ monic.

If $d_\ell - d_m \geq k + 1$ for some $\ell > m$, define

$$\tilde{f}_\ell = f_\ell - x^{d_\ell - d_m}f_m.$$

Clearly, $x^{d_\ell - d_m} \in A$, hence $\tilde{f}_\ell \in a$, because $f_\ell$ and $f_m$ are in $a$. Furthermore

$$\tilde{f}_\ell \notin \langle f_1, \ldots, f_{\ell-1} \rangle.$$

However, $\tilde{f}_\ell$ has smaller degree than $f_\ell$ because its leading term is 0.

The same argument works if $d_\ell = d_m$ for some $\ell \neq m$.

However, one of the two cases above must be satisfied. Indeed, if the $d$’s are distinct, then

$$d_1 < d_2 < \ldots < d_\ell < \ldots$$

is an increasing sequence, but then $d_{k+1} - d_1 \geq k + 1$. 