Part A: All Students

Hand in the following exercises from Chapter 11 of Artin’s book.

3.4 Observe that \( x - 1 \mapsto t \) so that \( f := (x - 1)^3 - 1 - y \) is in the kernel \( K \). I claim that \( K = \langle f \rangle \).

Clearly, \( \langle f \rangle \subseteq K \) since any multiple of \( f \) is also mapped to 0. Suppose \( g \in K \) is in the kernel. Since \( f \) is monic in \( y \), we can perform division with remainder to get \( g = fg + r \) where \( r \) has degree 0 in \( y \) so it must be a polynomial in \( x \) only, \( r = r(x) \). By hypothesis \( r(x) \mapsto r(t + 1) = 0 \), which happens only when \( r = 0 \). Hence \( f \) divides \( g \) so that \( g \in \langle f \rangle \). Hence \( K \subseteq \langle f \rangle \), so we have \( K = \langle f \rangle \).

Let \( I \) be an ideal which contains \( K = \langle f \rangle \). Then \( I \cap \mathbb{C}[x] \subseteq \mathbb{C}[x] \) is also an ideal, and by Prop. 11.3.22, \( \mathbb{C}[x] \) is a principle ideal so there exists \( g \in \mathbb{C}[x] \) such that \( I \cap \mathbb{C}[x] = \langle g \rangle \). I claim \( I = \langle f, g \rangle \).

Clearly we just need to prove \( I \subseteq \langle f, g \rangle \). Let \( h \in I \) and as before we can write \( h = fq + r \) for some polynomial \( r = r(x) \). Then \( r \in I \cap \mathbb{C}[x] \) so that \( r \in \langle g \rangle \) by hypothesis. Hence \( fq + r \in \langle f, g \rangle \) so \( h \in \langle f, g \rangle \).

3.5 (a) It’s clear from the definition that \((f + g)' = f' + g'\). Hence for the first part it suffices to prove the statements when \( f, g \) are monomials. Let \( f(x) = a_nx^n \) and \( g(x) = b_mx^m \).

\[
(fg)' = (a_n b_m x^{n+m})' = (n + m) a_n b_m x^{n+m-1} = na_n x^{n-1} b_m x^m + ma_n x^n b_m x^{m-1} = f'g + fg'
\]

For the second part we can assume \( f(x) = a_n x^n \) is a monomial and \( g(x) = b_m x^m + \cdots + b_1 x + b_0 \). We have \((f \circ g)' = (a_n g^n)'\). Note \( g^n \) is a product of many \( g \)'s, so apply the product rule inductively to get \((a_n g)^n' = na_n g^{n-1} g'\). Since \( f'(x) = na_n x^{n-2} \), we have \( f' \circ g = na_n g^{n-1} \) so the result follows.

(b) \( \Rightarrow \) Suppose \( \alpha \) is a multiple root of \( f \). Then we can write \( f(x) = (x - \alpha)^n g(x) \) for some \( g \in F[x] \) such that \( g(\alpha) \neq 0 \) and integer \( n > 1 \). By (a), \( f'(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n g'(x) \) so it’s clear \( f'(\alpha) = 0 \).

\( \Leftarrow \) Suppose \( \alpha \) is a common root of both \( f, f' \). Again write \( f(x) = (x - \alpha)^n g(x) \) where this time we only know \( n \geq 1 \) a priori. But then \( f'(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n g'(x) \) has \( \alpha \) as a root if and only if \( n > 1 \). Hence \( n > 1 \) we get a multiple root.

3.8 Let \( f : R \to R, f(x) = x^p \) be the Frobenius map. Then \( f(1) = 1^p = 1, f(xy) = (xy)^p = x^py^p = f(x)f(y) \), and finally

\[
f(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p = f(x) + f(y)
\]

where the middle equality is due to the fact that \( p \mid \binom{p}{i} \) whenever \( i \neq 0, p \). Hence \( f \) is a homomorphism.

3.11 False. Let \( R = \mathbb{Z} \) and \( I = \langle 2x \rangle \). Then \( n = 1 \) but \( I \) does not contain any monic degree one polynomial (the leading coefficient is always even).

3.12 We have \( 0 = 0 + 0 \in I + J \) and suppose \( a, b \in I + J \) where \( a = u + v, b = x + y \) and \( u, x \in I, v, y \in J \). Then \( a + b = (u + x) + (v + y) \in I + J \) and if \( r \in R \), then \( ra = ru + rv \in I + J \). Hence \( I + J \) is an ideal.
3.13 We have \(0 \in I \cap J\) and suppose \(a, b \in I \cap J\) so \(a + b \in I\) and \(a + b \in J\). Then \(a + b \in I \cap J\) and if \(r \in R\), then \(ra \in I \cap J\). Hence \(I \cap J\) is an ideal.

Consider \(R = \mathbb{Z}[t]\) and \(I = (3, t), J = (2, t)\). Then \(3t, 2t \in \{xy \mid x \in I, y \in J\}\) but \(3t - 2t = t \notin \{xy \mid x \in I, y \in J\}\) since \(t\) is irreducible and \(1 \notin I, J\).

We have \(0 \in IJ\) and suppose \(a, b \in IJ\). Then \(a + b \in IJ\) since the sum of two finite sums of products of elements in \(I, J\) is still a finite sum of products, and if \(r \in R\), then \(ra \in IJ\) since \(r \sum x \nu y \nu = \sum (rx \nu) y \nu\).

Note that \(IJ \subseteq I \cap J\) since any product \(xy\) belongs to both \(I\) and \(J\). However equality does not always hold, for example consider \(R = \mathbb{Z}, I = J = (2)\).

**Part B:** Math 563 Students

1. Let \(G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) be the Klein group. Write out the regular representation \(\rho: G \to \text{GL}(\mathbb{C}^4)\), using the standard basis of \(\mathbb{C}^4\).

2. Let \(G\) be a finite abelian group. Show that the number of distinct (i.e. pairwise non-isomorphic) representations of degree 1 of \(G\) equals the order of \(G\).

**1.** Let \(G = \{1, a, b, ab\}\) represent a basis for \(\mathbb{C}^4\). Then

\[
\rho(1) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

\[
\rho(a) = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

\[
\rho(b) = \begin{pmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix}
\]

\[
\rho(ab) = \begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{pmatrix}
\]

**2.** A degree 1 representation of \(G\) is a morphism \(\rho: G \to \mathbb{C}^\times\). Suppose \(G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}\) with generators \(a_1, \ldots, a_s\). Then \(\rho\) is uniquely determined by \(\rho(a_i)\) for \(i = 1, \ldots, s\). Observe \(\rho(a_i) = e^{2\pi ib_i/n_i}\) where \(b_i = 1, \ldots, n_i\). There are \(n_i\) choices for each \(b_i\) so gives us a total of \(|G|\) many representations. We show none of these are isomorphic. Let \(\rho, \rho'\) be two representations and \(\alpha: \mathbb{C} \to \mathbb{C}\) an isomorphism from \(\rho\) to \(\rho'\). Then \(\alpha(\rho(a_i)x) = b_i\alpha(x)\) and \(\rho'(a_i)\alpha(x) = b'_i\alpha(x)\). Hence \(b_i = b'_i\) for each \(i\) so \(\rho = \rho'\).