Solutions Ark2

From the book: Number 10, 11 and 12 on page 32.

**Number 10 :** Let $A$ be a ring, $\mathfrak{a}$ an ideal contained in the Jacobson radical of $A$; let $M$ be an $A$-module and $N$ a finitely generated $A$-module, and let $u : M \to N$ be homomorphism. If the induced homomorphism $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, then $u$ is surjective.

**Solution:** Let $\bar{u}$ denote the induced homomorphism. Then $\text{Im}\, \bar{u} = \text{Im}(u + \mathfrak{a}N)/\mathfrak{a}N$ (since $\bar{u}(\bar{m}) = \bar{n}$ means that $u(m) - n \in \mathfrak{a}$). So if $\bar{u}$ is surjective, $\text{Im}\, u + \mathfrak{a} = N$, and we can apply version 2.7 of *Nakayama’s* lemma and conclude that $\text{Im}\, u = N$, i.e., $u$ is surjective. $\blacksquare$

**Number 11 :** Let $A$ be a ring. Show that if $A^m \approx A^n$, then $m = n$. If $A^m \to A^n$ is surjective, then $m \geq n$. If $A^m \to A^n$ is injective, is it always true that $m \leq n$?

**Solution:** Let $m \subseteq A$ be a maximal ideal, and look at the induced map $(A/m)^m \to (A/m)^n$ which also is an isomorphism. Now $A/m$ is a field, and the isomorphism is an isomorphism of finite dimensional vector spaces which consequently must have the same dimension. Hence $m = n$.

If the map $A^m \to A^n$ is surjective, it follows immediately that $(A/m)^m \to (A/m)^n$ is a surjective map between finite dimensional vector spaces, hence $m \geq n$.

The last one is in fact always true, but I do not know a proof that can be given at this stage of the course. **Warning:** There are several proofs on the web, but the ones I have checked are either flawed or incomplet.$\blacksquare$

**Number 12 :** Let $M$ be a finitely generated $A$ module and $\phi : M \to A^n$ a surjective homomorphism. Show that $\text{Ker}\, \phi$ is finitely generated.

**Solution:** Let $e_1, \ldots, e_n$ be a basis for $A^n$ and let $u_i$ be elements in $M$ with $\phi(u_i) = e_i$. We shall see that $M$ is the direct sum of $\text{Ker}\, \phi$ and the submodule $N$ generated by $u_1, \ldots, u_n$. This will do, because then there is projection map $M \to \text{Ker}\, \phi$ which is surjective, and images of the generators of $M$ under this map will generate $\text{Ker}\, \phi$.

Now, $\text{Ker}\, \phi \cap N = 0$ for if $\phi(\sum a_iu_i) = \sum a_i e_i = 0$, it follows that each $a_i = 0$ since the $e_i$’s form a basis for $A^n$. On the other hand if $u \in M$ we may write $\phi(u) = \sum a_i e_i.$ Then $u - \sum a_iu_i \in \text{Ker}\, \phi$, so $M = N + \text{Ker}\, \phi$. And the two conditions $M = N + \text{Ker}\, \phi$ and $\text{Ker}\, \phi \cap N = 0$ are what we need to ensure $M$ being the direct sum of $N$ and $\text{Ker}\, \phi$. $\blacksquare$

**Oppgave 1.** Let $A$ be a ring and let $M$, $M'$, $N$ and $N'$ be four $A$-modules.
Show that \( \text{Hom}_A(M \oplus M', N) \cong \text{Hom}_A(M, N) \oplus \text{Hom}_A(M', N) \) and that \( \text{Hom}_A(M, N \oplus N') \cong \text{Hom}_A(M, N) \oplus \text{Hom}_A(M, N') \).

**Solution:** Let \( i : M \to M \oplus M' \) be the homorphism \( i(m) = (m, 0) \) and \( i' : M' \to M \oplus M' \) the one given by \( i'(m') = (0, m') \). Then we get a homorphism \( \phi \mapsto (\phi i, \phi i') \) from \( \text{Hom}_A(M \oplus M', N) \) to \( \text{Hom}_A(M, N) \oplus \text{Hom}_A(M', N) \).

It is injective since any element of \( M \oplus M' \) is of the form \( (m, m') = i(m) + i'(m') \), so if both \( \phi(i) = 0 \) and \( \phi(i') = 0 \), it follows that \( \phi = 0 \).

On the other hand, if \( \phi : M \to N \) and \( \phi' : M' \to N \) are given, the map \( \Phi(m, m') = \phi(m) + \phi'(m') \) maps to the pair \( (\phi, \phi') \).

The second part of the exercise is done in a similar manner, but using the projection maps \( \pi : M \oplus M' \to M \) and \( \pi' : M \oplus M' \to M' \) given by \( \pi(m, m') = m \) and \( \pi'(m, m') = m' \). They induce a map \( \phi \mapsto (\pi \phi, \pi' \phi) \) which one checks is an isomorphism.

**Oppgave 2.** If \( a \) and \( b \) are ideals in the ring \( A \) and \( a + b = A \), then \( (b : a) = b \).

**Solution:** Since \( a + b = A \) there are elements \( a \in a \) and \( b \in b \) such that \( a + b = 1 \). So if \( fb \subseteq b \), then \( f = fa + fb \in b \). Hence \( (b : a) \subseteq b \). The other inclusion is obvious (it follows from \( b \) being an ideal).

**Oppgave 3.** Show that we have \( \text{Hom}_A(A/a, A/b) = (b : a)/b \). Show further that \( \text{Hom}_A(A/(x)A, A) = \text{Ann}(x) \) for an element \( x \in A \).

**Solution:** An \( A \)-homomorphism \( \phi \) from \( A \) to any \( A \)-module is given by the element \( m = \phi(1) \in M \); indeed \( \phi(a) = a\phi(1) = am \) since \( \phi \) is \( A \)-linear. There is no restriction on \( m \), any element in \( M \) gives a homomorphism.

An \( A \)-homomorphism \( \phi \) from \( A/a \) to \( M \) is also given by \( m = \phi(\bar{1}) \), because \( \phi(a) = a\phi(1) \). But now there are conditions on \( m \). Since \( \bar{a} = 0 \) whenever \( a \in a \), we must have \( a\phi(\bar{1}) = 0 \) for all \( a \in a \). From the fundamental theorem on quotients, it follows that this is the only condition. Hence \( \text{Hom}_A(A/a, M) \approx \{ m \in M \mid am = 0 \} \).

Putting \( M = A/b \), we we have \( \text{Hom}_A(A/a, A/b) \approx \{ y \in A/b \mid ay = 0 \} = \{ x \mid x \in A \text{ and } a\bar{x} \in b \} = (b : a)/b \).

**Oppgave 4.** If \( a \) and \( b \) are two comaximal ideals, then \( \text{Hom}_A(A/a, A/b) = 0 \).

**Solution:** This follows directly from the two previous exercises: We have \( (b, a) = b \) and therefore \( \text{Hom}_A(A/a, A/b) = (b : a)/b = 0 \).

**Oppgave 5.** Determine \( \text{Hom}_\mathbb{Z}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \), \( \text{Hom}_\mathbb{Z}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}) \) and \( \text{Hom}_\mathbb{Z}(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}) \).
SOLUTION: We use the previous exercise:

Hom\(_{\mathbb{Z}}(\mathbb{Z}/8\mathbb{Z},\mathbb{Z}/2\mathbb{Z}) \approx \mathbb{Z}/2\mathbb{Z}\) because any element in \(\mathbb{Z}/2\mathbb{Z}\) is killed by 8. Furthermore, Hom\(_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/8\mathbb{Z}) \approx 4\mathbb{Z}/8\mathbb{Z}\), i.e., the ideal generated by 4 in \(\mathbb{Z}/8\mathbb{Z}\), this because any integer \(x\) such that \(2x\) is divisible by 8 must be divisible by 4.

Finally, Hom\(_{\mathbb{Z}}(\mathbb{Z}/4\mathbb{Z},\mathbb{Z}/8\mathbb{Z}) \approx 2\mathbb{Z}/8\mathbb{Z}\), i.e., the ideal generated by 2 in \(\mathbb{Z}/8\mathbb{Z}\), again because if \(4x\) is divisible by 8 for an integer \(x\), then \(x\) is divisible by 2. □

OPPGAVE 6. What is Hom\(_{\mathbb{Z}}(\mathbb{Z}/55\mathbb{Z},\mathbb{Z}/121\mathbb{Z})\)? What about Hom\(_{\mathbb{Z}}(\mathbb{Z}/55\mathbb{Z},\mathbb{Z}/565\mathbb{Z})\)?

SOLUTION: We have \(55 = 5 \times 11\) and \(121 = 11^2\). Hence \(\mathbb{Z}/55\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}\), We get Hom\(_{\mathbb{Z}}(\mathbb{Z}/55\mathbb{Z},\mathbb{Z}/121\mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z},\mathbb{Z}/121\mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z},\mathbb{Z}/121\mathbb{Z}) \oplus \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/11\mathbb{Z},\mathbb{Z}/121\mathbb{Z})\) since 5 and 11 are relatively prime.

Now Hom\(_{\mathbb{Z}}(\mathbb{Z}/11\mathbb{Z},\mathbb{Z}/121\mathbb{Z}) \approx 11\mathbb{Z}/121\mathbb{Z} \approx \mathbb{Z}/11\mathbb{Z}\) since an integer \(x\) with \(11x\) divisible by 121 must be divisible by 11. □

OPPGAVE 7. If \(k\) is a field, then Hom\(_k(k^n, k^m) \approx M_{n,m}(k)\) where \(M_{n,m}(k)\) stands for the vectorspace of \(m \times n\)-matrices with entries in \(k\).

SOLUTION: This is just linear algebra! □

OPPGAVE 8. Determine Hom\(_{\mathbb{Z}}(\mathbb{Z}[i],\mathbb{Z}[i])\) and Hom\(_{\mathbb{Z}[i]}(\mathbb{Z}[i],\mathbb{Z}[i])\).

SOLUTION: In general it is true that for a ring \(A\) and an \(A\)-module \(M\) we have Hom\(_{A}(A, M) \approx M\). The isomorphism is given by sending \(\phi\) to \(\phi(1)\) (this is certainly a very natural isomorphism and merits to be called "canonical"). That the homomorphism \(\phi\) is determined by \(\phi(1)\) follows since \(\phi\) being \(A\)-linear gives \(\phi(a) = a\phi(1)\). On the other hand, posing \(\phi(a) = am\) gives a homomorphism, for any choice of \(m\) from \(M\). Hence Hom\(_{\mathbb{Z}[i]}(\mathbb{Z}[i],\mathbb{Z}[i]) \approx \mathbb{Z}[i]\).

For the other homomorphism group — Hom\(_{\mathbb{Z}}(\mathbb{Z}[i],\mathbb{Z}[i]) — we are looking at \(\mathbb{Z}\)-module homomorphisms, i.e., group homomorphism (so we are ignoring the multiplicative structure on \(\mathbb{Z}[i]\)). As an abelian group \(\mathbb{Z}[i]\) is free of rank two, i.e., \(\mathbb{Z}[i] \approx \mathbb{Z}^2\). Hence Hom\(_{\mathbb{Z}}(\mathbb{Z}[i],\mathbb{Z}[i]) \approx \mathbb{Z}^4\). (By oppgave 1 above and the remark at the beginning of this exercise.)

One may identify Hom\(_{\mathbb{Z}[i]}(\mathbb{Z}[i],\mathbb{Z}[i])\) with the subgroup of Hom\(_{\mathbb{Z}}(\mathbb{Z}[i],\mathbb{Z}[i])\) consisting of those additive (i.e., \(\mathbb{Z}\)-linear) maps which also respects the multiplication. It is easy to see that an additive map \(\phi\) is among the multiplicative ones if and only if \(\phi(i) = i\phi(1)\).

One may identify Hom\(_{\mathbb{Z}}(\mathbb{Z}[i],\mathbb{Z}[i])\) with the additive group of \(2 \times 2\) matrices with entries in \(\mathbb{Z}\) (which is also a ring, with multiplication corresponding to composition of
maps), i.e., with the set of matrices
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]
with \(a, b, c\) and \(d\) in \(\mathbb{Z}\).

The subgroup (or even subring) of matrices corresponding to maps in \(\text{Hom}_{\mathbb{Z}[i]}(\mathbb{Z}[i], \mathbb{Z}[i])\) are the ones of the form
\[
\begin{pmatrix}
a & b \\
-b & a
\end{pmatrix}
\]
with \(a\) and \(b\) \(\in\) \(\mathbb{Z}\).

**Oppgave 9.** Let \(K\) be a field and let \(A \subset K\) be a local ring which is not a field. Show that \(K\) can not be a finitely generated \(A\)-module.

Let \(B \subset K\) be a ring which is not a field. Show that \(K\) is not finitely generated as an \(B\)-module (HINT: If \(m \subset B\) is a maximal ideal, let \(A = \{a/b \mid b \not\in m\}\). Show that \(A\) is a local ring with maximal ideal \(mA\). This is a special case of a general construction we shall do later on).

**Solution:** This is an application of Nakayama’s lemma. If \(A\) is a local ring which is not a field, it has a non-zero maximal ideal \(m\). And clearly \(mK = K\) since non-zero elements in \(K\) are invertible. If \(K\) were finitely generated over \(A\), Nakayama would tell us that \(K = 0\) which is not the case.

In the second part, let \(m\) be a maximal ideal in \(A\) and replace \(A\) by the localisation \(A_m\).

**Oppgave 10.** Let \(M\) be a finitely generated \(A\)-module and \(\phi : M \rightarrow M\) a \(A\)-homomorphism. If \(\phi\) is surjective, then \(\phi\) is an isomorphism. (HINT: Regard \(M\) as a module over the polynomial ring \(A[X]\) by letting \(X\) act on \(M\) as \(\phi\), i.e., \(Xm = \phi(m)\) for \(m \in M\). Then use Corollary 2.5 with \(a = (X)A[X]\).)

**Solution:** As hinted, we regard \(M\) as a module over the ring of polynomials \(A[X]\), by letting \(Xm := \phi(m)\). (Hence a polynomial \(\sum a_iX^i\) acts as \((\sum a_iX^i).m = \sum a_i\phi^i(m)\).) Certainly \(M\) is finitely generated over \(A[X]\) — generators over \(A\) are also generators over the bigger ring.

Furthermore let \(a = (X)A[X]\). Since \(\phi\) is surjective, \(XM = M\) and thence \(aM = M\). By version 2.5 of Nakayama, we can find an element \(x\) killing \(M\) with \(x \equiv 1 \mod a\), that is \(x = 1 + P(X)X\) for some polynomial \(P(X)\). But as \(xM = 0\), it follows that \(id_M = -P(\phi)\phi\), and consequently \(-P(\phi)\) is an inverse map to \(\phi\).

**Oppgave 11.** Use Zorn’s lemma to show that any finitely generated module has a maximal, proper submodule. Use this to give another proof of Nakayama’s lemma.
Give an example of a module — necessarily not finitely generated — without maximal, proper submodules.

**Solution:** Let \( \{ M_i \}_{i \in I} \) be an ascending chain of proper submodules (which are not necessarily finitely generated). We shall see that the union \( \bigcup_{i \in I} M_i \) is a proper submodule.

Indeed, assume \( M = \bigcup_{i \in I} M_i \) and let \( m_1, \ldots, m_r \) be generators for \( M \). Then each \( m_i \) lies in \( M_{\rho(i)} \) for some \( i \in I \), and hence in \( M_j \) for \( j \geq \rho(i) \) as the chain is ascending. One of the \( M_i \)'s therefore contains all of the generators \( m_i \). This is not the case since all the \( M_i \)'s were supposed to be proper submodules, and the union is a proper submodule.

By Zorn’s lemma we conclude that there exists a maximal, proper submodule.

To derive Nakayama from this, let \( N \) be such a maximal, proper submodule. Pick an \( e \in M \) but \( e \notin N \). Now the module \( <e> = Ae \) generated by \( e \), contains \( e \) and hence is not contained in \( N \). Since \( N \) is maximal, proper, it follows that \( M = Ae + N \). If now \( aM = M \), we get \( e = ae + n \) for some \( a \in \mathfrak{a} \) and some \( n \in N \). Thus \( (1-a)e \in N \), and as \( a \) is contained in the Jacobson-radical, \( (1-a) \) is invertible, and \( e \in N \). Contradiction. \( \square \)

**Oppgave 12.** The aim of this exercise is to investigate the behavior of a prime ideal \((p)\mathbb{Z}\) when extend to the ring of Gaussian integers \( \mathbb{Z}[i] \). Throughout the exercise \( p \) will be a prime.

Recall that \( \mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i] \) with \( X \) corresponding to \( i \).

a) Show that \( \mathbb{Z}[i]/(p)\mathbb{Z}[i] \cong \mathbb{F}_p[X]/(X^2 + 1) \) with \( X \) corresponding to \( i \). (Hint: Both are isomorphic to \( \mathbb{Z}[X]/(p, X^2 + 1) \).)

**Solution:** The map \( \phi : \mathbb{Z}[X] \to \mathbb{Z}[i] \) given by \( X \mapsto i \), identifies \( \mathbb{Z}[i] \) with the quotient \( \mathbb{Z}[X]/(x^2 + 1) \). Now \( \phi^{-1}(p\mathbb{Z}[i]) = (p, X^2 + 1) \). Hence \( \mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{Z}[X]/(p, X^2 + 1) \). On the other hand \( \mathbb{Z}[X]/(p, X^2 + 1) \approx \mathbb{F}_p[X]/(x^2 + 1) \) as \( \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \). \( \square \)

There are three cases:

i) **The case \( p = 2 \).**

In this case show that \( X^2 + 1 = (X + 1)^2 \) in \( \mathbb{F}_2[X] \) and hence the equality \( (2) = (i + 1)^2 \) of ideals in \( \mathbb{Z}[i] \). (Which one of course also can see directly).

**Solution:** Over \( \mathbb{F}_2 \) we have \( (X + 1)^2 = X^2 + 2X + 1 = X^2 = 1 \) since \( 2 = 0 \) in \( \mathbb{F}_2 \). The map \( \mathbb{Z}[i]/2\mathbb{Z}[i] \to \mathbb{F}_2[X]/((X+1)^2) \mathbb{F}_2[X] \) where \( i \mapsto X \) shows that \( (2)\mathbb{Z}[i] = (i+1)^2\mathbb{Z}[i] \). (Or directly, using that \( (1+i)^2 = 2i \); \( (i+1)^2\mathbb{Z}[i] = (2i)\mathbb{Z}[i] = (2)\mathbb{Z}[i] \) since \( i \) is invertible in \( \mathbb{Z}[i] \). \( \square \)

ii) **The case when \(-1\) is square mod \( p \).**

— 5 —
Then the polynomial \( X^2 + 1 \) has a root in \( \mathbb{F}_p \), say the residue class \( \bar{n} \) of an integer \( n \). Hence \( X^2 + 1 = (X - \bar{n})(X + \bar{n}) \). Show that \((p)[i] = (i - n, p) \cap (i + n, p) \) and that those two ideals both are prime.

**Solution:** In this case we have the equality \((X^2 + 1)\mathbb{F}_p[X] = (X - \bar{n})\mathbb{F}_p[X] \cap (X + \bar{n})\mathbb{F}_p[X]\) of ideals in \( \mathbb{F}_p[X] \), so the \((p, X^2 + 1)\mathbb{Z}[X] = (p, X - n)\mathbb{Z}[X] \cap (p, X + n)\mathbb{Z}[X]\) and thus \((p)[i] = (p, X - n)\mathbb{Z}[i] \cap (p, X + n)\mathbb{Z}[i]\).

The ideal \((p, X - n)\) is prime, because

\[ \mathbb{Z}[i]/(p, X - n) \approx \mathbb{Z}[X]/(p, X^2 + 1, X - n) \approx \mathbb{F}_p[X]/(X^2 + 1, X - \bar{n}) \approx \mathbb{F}_p \]

since \( X^2 + 1 = (X - \bar{n})(X + \bar{n}) \) in \( \mathbb{F}_p[X] \). Now \( \mathbb{F}_p \) is a field and hence \((p, X - n)\) is a maximal ideal.

iii) **The case \(-1\) is not a square mod \(p\).**

In this case \( X^2 + 1 \) is irreducible in \( \mathbb{F}_p[X] \) and \((X^2 + 1)\) is a prime ideal. Use this to show that \((p)[i] X \) is prime.

**Solution:** Since \( \mathbb{Z}[X]/(p)[i] \approx \mathbb{F}_p[X]/(X^2 + 1), \) and the latter is an integral domain since \( X^2 + 1 \) is irreducible in \( \mathbb{F}_p[X] \), it follows that \((p)[i] \) is prime. (In fact both ideals are maximal).

iv) Here we go further and analyse when cases ii) and iii) occure, i.e., we shall give a criterion for a prime, which we assume different from 2, to have the property that \(-1\) is a square mod \(p\). Recall that \( \mathbb{F}_p^* \) denotes the multiplicative group of non zero elements in the finite field \( \mathbb{F}_p \), and that this group is cyclic of order \( p - 1 \). (Every finite subgroup of the group of units in field is cyclic. This is a theorem).

Let \( \sigma : \mathbb{F}_p^* \to \mathbb{F}_p^* \) be the map sending \( x \) to \( x^\frac{p-1}{2} \), and let \( \tau \) be the one sending \( x \) to \( x^\frac{p-1}{2} \). Show that there is an exact sequence

\[
\begin{array}{c}
1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^* \xrightarrow{\sigma} \mathbb{F}_p^* \xrightarrow{\tau} \mathbb{F}_p^* \xrightarrow{\tau} \mathbb{F}_p^* \\
\end{array}
\]

meaning that the kernel \( \text{Ker} \sigma = \{\pm 1\} \) and that \( \text{Ker} \tau = \text{Im} \sigma \). Conclude that \(-1\) is a square mod \(p\) if and only if \((p - 1)/2\) is even, i.e., \(p \equiv 1 \mod 4\).

**Solution:** One has \( \tau \sigma = 1 \) (we are working with multiplicative, abelian groups, and the constant homomorphism \( x \mapsto 1 \) plays the role as the “zero” map), since

\[
(x^2)^\frac{p-1}{2} = x^{p-1} = 1 \quad \text{— taken into account that} \quad \mathbb{F}_p^* \quad \text{is cyclic of order} \quad p - 1.
\]

In a field the equation \( X^2 - 1 = 0 \) has only \( \pm 1 \) solutions, hence \( \text{Ker} \sigma = \{\pm 1\} \).

Now \( \tau(t) \neq 1 \) since the order of \( \mathbb{F}_p^* \) is \( p - 1 \) and \( \not= \frac{p-1}{2} \). Clearly it takes values in \( \{\pm 1\} \), so the kernel has order \( \frac{p-1}{2} \). But this is exactly the order of \( \text{Im} \sigma \), since \( |\text{Im} \sigma| = |\mathbb{F}_p^*|/|\text{Ker} \sigma| = (p - 1)/2 \). Consequently, \( \text{Im} \sigma = \text{Ker} \tau \).