Jendrik Stelzner Last changed: November 28, 2018

Algebra II, Sheet 6

Remarks and Solutions

Exercise 1.

For every multiindex $\mu = (\mu_1, \dots, \mu_n)$ we denote by $x^\mu \in k[x_1, \dots, x_n]$ the element

$$x^\mu \coloneqq x_1^{\mu_1} \cdots x_n^{\mu_n} \,.$$

(a)

For every $f \in k[x_1, \dots, x_n]$ the element

$$f' \coloneqq \sum_{g \in G} g.f$$

is G-invariant because

$$g.f' = g. \sum_{g' \in G} g'.f = \sum_{g' \in G} gg'.f = \sum_{g'' \in G} g''.f = f \,.$$

For every multiindex $\mu = (\mu_1, \dots, \mu_n)$ we choose $f = x^\mu$, and thus set

$$J_\mu \coloneqq \sum_{g \in G} g.x^\mu \,.$$

(b)

It holds for every G-invariant $f \in k[x_1, \dots, x_n]^G$ that

$$\sum_{g \in G} g.f = \sum_{g \in G} f = |G| f \,.$$

But with $f = \sum_\mu a_\mu x^\mu$ it also holds that

$$\sum_{g \in G} g.f = \sum_{g \in G} g. \sum_\mu a_\mu x^\mu = \sum_\mu a_\mu \sum_{g \in G} g.x^\mu = \sum_\mu a_\mu J_\mu \,.$$

Remark 1. If $\operatorname{char}(k) \nmid |G|$ and V is any representation of G over k then the map

$$R\colon V \to V\,, \quad v \mapsto \frac{1}{|G|} \sum_{g \in G} g.v$$

is a projection of V onto the subspace of invariants $V^G \subseteq V$. This projection is known as the *Reynolds operator*.

(c)

Let $h \coloneqq |G|$ and let $G = \{g_1, \dots, g_h\}$.

It follows from the previous part of the exercise that $k[x_1, \dots, x_n]$ is generated by the G-invariants J_μ as a vector space, where $\mu \in \mathbb{N}^n$, because the factor $|G|$ is invertible in k. It therefore sufficies to show that every J_μ can be written as polynomial in those J_ν for which $|\nu| \leq h$.

For every $j \geq 0$ let $p_j = Y_1^j + \cdots + Y_h^j \in k[Y_1, \dots, Y_h]$ be the j-th power symmetric polynomial. For the elements

$$y_i \coloneqq (g_i.x_1)Z_1 + \cdots + (g_i.x_n)Z_n \in k[x_1, \dots, x_n][Z_1, \dots, Z_n]$$

with $i = 1, \dots, h$ we then have that

$$\begin{aligned}
p_j(y_1, \dots, y_h) &= y_1^j + \cdots + y_h^j \\
&= \sum_{i=1}^h \bigl[(g_i.x_1)Z_1 + \cdots + (g_i.x_n)Z_n\bigr]^j \\
&= \sum_{i=1}^h \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} [(g_i.x_1)Z_1]^{\mu_1} \cdots [(g_i.x_n)Z_n]^{\mu_n} \\
&= \sum_{i=1}^h \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} (g_i.x_1)^{\mu_1} \cdots (g_i.x_n)^{\mu_n} Z^\mu \\
&= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} \left[\sum_{i=1}^h (g_i.x_1)^{\mu_1} \cdots (g_i.x_n)^{\mu_n}\right] Z^\mu \\
&= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} \left[\sum_{i=1}^h g_i.x^\mu\right] Z^\mu \\
&= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} J_\mu Z^\mu\,.
\end{aligned}$$

This shows that J_μ is, up to the factor

$$C_\mu \coloneqq \binom{|\mu|}{\mu_1, \dots, \mu_n}\,,$$

the coefficient of the monomial Z^μ in $p_j(y_1, \dots, y_n)$.

We know that for every $j > h$ the j-th power symmetric polynomial p_j can be expressed as a k-polynomial in the power symmetric polynomials $p_1, \dots, p_h$ because $\operatorname{char}(k) = 0$. It follows that the coefficients of $p_j(y_1, \dots, y_n)$ are k-polynomials in the coefficients of $p_1(y_1, \dots, y_n), \dots, p_h(y_1, \dots, y_n)$.

This shows for every multiindex μ that the G-invariant $C_\mu J_\mu$ can be expressed as a k-polynomial in the G-invariants $C_\nu J_\nu$ with $|\nu| \leq h$. The factor C_μ is invertible in k, hence every J_μ is a k-polynomial in those J_ν with $|\nu| \leq h$.

Remark 2. Let V be a finite-dimensional of a finite group G over k. The *Noether number of V* is given by

$$\beta(V, G) = \inf\{d \geq 0 \mid \mathcal{P}(V)^G \text{ is generated by homogeneous elements of degree } \leq d\},$$

and the *Noether number of G* is given by

$$\beta(G) \coloneqq \sup\{\beta(V, G) \mid V \text{ is a finite-dimensional representation of } G \text{ over } k\}.$$

Noether's theorem (1915) shows that $\beta(G) \leq |G|$ if $\operatorname{char}(k) = 0$, which is known as the *Noether bound*. This result can be strengthened in various ways:

- Fogarty (2001) showed that that the Noether bound holds under the weaker assumption that $\operatorname{char}(k) \nmid |G|$.
- Fleischmann (2000) showed the more general result that if $H \subseteq G$ is a normal subgroup with $\operatorname{char}(k) \nmid [G : H]$, then $\beta(V, G) \leq \beta(V, H) \cdot [G : H]$.
- Schmid (1991) showed for $\operatorname{char}(k) = 0$ that $\beta(G) \leq \beta(H)[G : H]$ for every subgroup $H \subseteq G$, and that $\beta(G) \leq \beta(H)\beta(G/H)$ if H is normal in G.
- It is an open problem if $\beta(G) \leq \beta(H)[G : H]$ holds for every subgroup $H \subseteq G$ under the weaker condition that $\operatorname{char}(k) \nmid [G : H]$.

Exercise 2.

(a)

Let more generally R be any ring and let M be an R-module. Recall that a submodule $N \subseteq M$ is *maximal* if it follows for every intermediate submodule $N \subseteq P \subseteq M$ that $P = N$ or $P = M$. This is equivalent to the quotient module M/N having precisely two submodules, i.e. equivalent to M/N being simple. It follows in particular that R/M is simple for every maximal left ideal $M \subseteq R$.

Every simple R-module S is already of this form. The module S is cyclic: It holds that $S \neq 0$ and for $x \in S$ with $x \neq 0$ the submodule $\langle x \rangle$ is a nonzero submodule of S. Hence $S = \langle x \rangle$ because S is simple. This shows that $S \cong R/M$ for some module M. The simplicity of S is by the above argumentation equivalent to M being maximal.

The maximal ideals in $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime. The simple $\mathbb{Z}$-modules are therefore (up to isomorphism) precisely $\mathbb{Z}/p\mathbb{Z}$ with p prime.

Remark 3. We have seen above that a simple module S is not only cyclic, but that every nonzero element $x \in S$ is already a cyclic generator. This is an equivalent characterization of simple modules: A module S is simple if and only if $S \neq 0$ and every nonzero $x \in S$ is a cyclic generator.

Indeed, if S satisfies this condition(s), then S contains no proper nonzero cyclic submodule, and hence no proper nonzero submodule. Since $S \neq 0$, this means that S is simple.

Warning 4. Different maximal ideals $M, M' \subseteq R$ may given isomorphic simple modules $R/M \cong R/M'$. An example for this is $R = \mathrm{M}_n(k)$ with $n \geq 2$ and k a field.

(b)

If R is an integral domain that is not a field then R not semisimple: It holds for any two nonzero ideals $I, J \subseteq R$ that $I \cap J \supseteq IJ \neq 0$, and hence that the sum $I + J$ is not direct. If $x \in R$ is a nonzero non-unit then this shows that the generated ideal $\langle x \rangle$ has no direct complement.

In particular $2\mathbb{Z} \subseteq \mathbb{Z}$ has no direct complement.

(c)

Every semisimple $\mathbb{Z}$-module M is by part (a) of the form

$$M \cong \bigoplus_{i \in I} \mathbb{Z}/p_i$$

for some primes p_i. The primes p_i are in particular square-free, which proves the statement.

Remark 5. One has for every $n \geq 0$ that $\mathbb{Z}/n$ is semisimple if and only if n is square-free. Indeed, if $n = 0$ then $\mathbb{Z}/n = \mathbb{Z}$ is not semisimple, and if $n = 1$ then $\mathbb{Z}/n = 0$ is semisimple. For $n \geq 2$ we have $n = p_1^{n_1} \cdots p_r^{n_r}$ for some pairwise different primes p_i and exponents $n_i \geq 1$. Then

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_r}$$

by the chinese reminder theorem. This is already a decomposition into indecomposable $\mathbb{Z}$-modules by the classification of finitely generated abelian groups. Hence $\mathbb{Z}/n$ is semisimple if and only if every summand $\mathbb{Z}/p_i^{n_i}$ is already simple. We have seen above that this is the case if and only if every $p_i^{n_i}$ is prime, i.e. if and only if $n_i = 1$ for every $i = 1, \ldots, r$.

It follows that a $\mathbb{Z}$-module M is semisimple if and only if $M \cong \bigoplus_i \mathbb{Z}/n_i$ where the n_i are square-free integers.

Exercise 3.

Recall the universal properties of the direct sum and the direct product:

- Let $(M_\alpha)_{\alpha \in A}$ be a collection of R-modules and let N be another R-module. For every $\alpha \in A$ let $i_\alpha \colon M_\alpha \to \bigoplus_{\beta \in A} M_\beta$ be the inclusion into the α-th summand.

  Then every choice of homomorphism $f_\alpha \colon M_\alpha \to N$ with $\alpha \in A$ can be uniquely extended to a homomorphism $f \colon \bigoplus_{\alpha \in A} M_\alpha \to N$, in the sense that $f \circ i_\alpha = f_\alpha$ for every $\alpha \in A$. The homomorphism f is given on elements by

  $$f\left((m_\alpha)_{\alpha \in A}\right) = \sum_{\alpha \in A} f_\alpha(m_\alpha)$$

  for every $(m_\alpha)_{\alpha \in A} \in \bigoplus_{\alpha \in A} M_\alpha$. Note that f is well-defined because $m_\alpha = 0$ for all but finitely many $\alpha \in A$, and hence also $f_\alpha(m_\alpha) = 0$ for all but finitely many $\alpha \in A$.

  This construction results in an isomorphism of abelian groups

  $$\operatorname{Hom}_R\left(\bigoplus_{\alpha \in A} M_\alpha, N\right) \longleftrightarrow \prod_{\alpha \in A} \operatorname{Hom}_R(M_\alpha, N)\,.$$

- Let M be an R-module and let $(N_\alpha)_{\alpha \in A}$ be a collection of R-modules. For every $\alpha \in A$ let $p_\alpha \colon \prod_{\beta \in A} N_\beta \to N_\alpha$ be the projection onto the α-th factor.

  Then every choice of homomorphism $f_\alpha \colon M \to N_\alpha$ with $\alpha \in A$ can be uniquely combined into a homomorphism $f \colon M \to \prod_{\alpha \in A} N_\alpha$, in the sense that $p_\alpha \circ f = f_\alpha$ for every $\alpha \in A$. The homomorphism f is given on elements by

  $$f(m) = (f_\alpha(m))_{\alpha \in A}$$

  for every $m \in M$.

  This construction results in an isomorphism of abelian groups

  $$\operatorname{Hom}_R\left(M, \prod_{\alpha \in A} M_\alpha\right) \longleftrightarrow \prod_{\alpha \in A} \operatorname{Hom}_R(M, N_\alpha)\,. \tag{1}$$

Warning 6. The isomorphism (1) does in general not restrict to an isomorphism

$$\operatorname{Hom}_R\left(M, \bigoplus_{\alpha \in A} M_\alpha\right) \longleftrightarrow \bigoplus_{\alpha \in A} \operatorname{Hom}_R(M, N_\alpha)\,.$$

But it does if M is finitely generated.

We now have that

$$R' = \operatorname{Hom}_{\mathbb{Z}}(E, E) = \operatorname{Hom}_{\mathbb{Z}}\left(\bigoplus_p \mathbb{Z}/p, \bigoplus_q \mathbb{Z}/q\right) \cong \prod_p \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \bigoplus_q \mathbb{Z}/q\right)$$

The inclusion $i \colon \bigoplus_q \mathbb{Z}/q \to \prod_q \mathbb{Z}/q$ induces an inclusion of abelian groups

$$\operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \bigoplus_q \mathbb{Z}/q\right) \xrightarrow{i_*} \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \prod_q \mathbb{Z}/q\right) \cong \prod_q \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/p, \mathbb{Z}/q)\,.$$

It follows from Schur's lemma that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p, \mathbb{Z}/q) = 0$ if $p \neq q$. (This can also be seen by looking at the p-torsion (or q-torsion) of both sides.) We have for $p = q$ that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p, \mathbb{Z}/p) = \mathrm{Hom}_{\mathbb{Z}/p}(\mathbb{Z}/p, \mathbb{Z}/p) = \mathrm{End}_{\mathbb{Z}/p}(\mathbb{Z}/p) \cong \mathbb{Z}/p\,.$$

Hence

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \prod_q \mathbb{Z}/q\right) \cong \mathbb{Z}/p\,,$$

where for $\lambda \in \mathbb{Z}/p$ the corresponding homomorphism is given by

$$\mathbb{Z}/p \xrightarrow{\lambda\cdot(-)} \mathbb{Z}/p \hookrightarrow \prod_q \mathbb{Z}/q\,.$$

Every such homomorphism restricts to a homomorphism $\mathbb{Z}/p \to \bigoplus_q \mathbb{Z}/q$, hence the above homomorphism i_* is already an isomorphism. We thus find that

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \bigoplus_q \mathbb{Z}/q\right) \cong \mathbb{Z}/p\,,$$

with the same description as above.

It follows that

$$R' \cong \prod_p \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/p, \bigoplus_q \mathbb{Z}/q\right) \cong \prod_p \mathbb{Z}/p\,,$$

where an element $(\lambda_p)_p \in \prod_p \mathbb{Z}/p$ acts on $(x_p)_p \in E$ via

$$(\lambda_p)_p \cdot (x_p)_p = (\lambda_p x_p)_p\,.$$

To determine R'' we use the following observation:

Lemma 7. Let R be a commutative ring and let M be an R-module. If $R' = \mathrm{End}_R(M)$ is again commutative then $R'' = R'$.

Proof. It follows from R being commutative that $R \subseteq R'$, and hence that $R' \supseteq R''$. It holds that $R' \subseteq R''$ because R' is commutative. □

We find that $R'' = R' = \prod_p \mathbb{Z}/p$. The (unique) ring homomorphism

$$\mathbb{Z} = R \to R'' = \prod_p \mathbb{Z}/p$$

is not surjective, so $R'' \neq R$.