Algebra - Spring 2012

Daren Cheng
Jesse Madnick

Last updated: September 2013

Acknowledgments & Disclaimers

Some of the solutions contained herein are my own, but many are not. I am indebted to Daren Cheng for sharing with me his solutions to several full-length exams. I'd also like to acknowledge Zev Chonoles, Fernando Shao, and my algebra professors Dan Bump and Akshay Venkatesh, all of whom patiently tolerated my many questions.

I am not exactly an algebraist. My writing style tends towards the wordy side, and my preferred proofs are rarely the most elegant ones. Still, I hope to keep these solutions free of any substantial errors. For this reason: if you notice any errors (typographical or logical), *please* let me know so I can fix it! Your speaking up would be a kindness for future students who may be struggling to make sense of an incorrect expression. I can be reached at jmadnick@math.stanford.edu.

1. Let R be a finite-dimensional algebra over a field k.

(a) Prove that if R is a commutative integral domain, then R is a field.

Solution: Let $r \in R$, $r \neq 0$. Let

$$\begin{aligned} m_r \colon R &\to R \\ x &\mapsto rx. \end{aligned}$$

Note that m_r is k-linear. Since R is an integral domain, m_r is injective. Thus, since R is a finite-dimensional k-vector space, m_r is surjective. Therefore, there exists $x \in R$ with $rx = 1$, which shows that $r \in R^\times$. Hence, R is a field.

Alternate Solution: Let $r \in R$, $r \neq 0$. Since R is a finite-dimensional k-algebra, Problem 8(a) implies that the ring extension $k \subset R$ is integral. Therefore, $r \in R$ satisfies a monic polynomial, say

$$r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 = 0, \quad a_i \in k.$$

Suppose this polynomial is of minimal degree. Since R is an integral domain, we have $a_0 \neq 0$. (If $a_0 = 0$, then we'd contradict minimality.) Subtracting a_0 from both sides, we have $r(r^{n-1} + a_{n-1}r^{n-2} + \ldots + a_1) = -a_0$, so

$$r \cdot -a_0^{-1}(r^{n-1} + a_{n-1}r^{n-2} + \ldots + a_1) = 1.$$

This shows that $s = -a_0^{-1}(r^{n-1} + a_{n-1}r^{n-2} + \ldots + a_1) \in R$ is an inverse for r.

(b) Suppose R is not commutative. Prove that $rs = 1$ implies $sr = 1$.

Solution: Let $r \in R$ have $rs = 1$. Let

$$\begin{aligned} m_r \colon R &\to R \\ x &\mapsto rx. \end{aligned}$$

Note that m_r is k-linear. Note that for any $y \in R$, we have $m_r(sy) = rsy = y$, so m_r is surjective. Thus, since R is a finite-dimensional k-vector space, m_r is injective. By injectivity, $m_r(sr) = rsr = r = m_r(1)$ implies that $sr = 1$.

2. Suppose A is a (commutative) ring, and M is an A-module.

(a) If $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A, must $M = 0$? Prove or disprove.

Solution: Yes. We prove the contrapositive: Suppose $M \neq 0$. Let $x \in M$, $x \neq 0$. Consider the ideal $\mathrm{Ann}(x) := \{a \in A \colon ax = 0\}$. Since $\mathrm{Ann}(x) \neq (1)$, there exists a maximal ideal $\mathfrak{m} \supset \mathrm{Ann}(x)$. We claim that $M_{\mathfrak{m}} \neq 0$.

Otherwise, if $M_{\mathfrak{m}} = 0$, then $x/1 = 0$, so there would exist $s \in A - \mathfrak{m}$ with $sx = 0$. That is, there would exist an $s \notin \mathfrak{m}$ with $s \in \mathrm{Ann}(x) \subset \mathfrak{m}$ – which is impossible. Thus, $M_{\mathfrak{m}} \neq 0$.

(b) If M is finitely generated and $M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A, prove that $M = 0$. Give a counterexample if M is not finitely generated.

Solution: Since M is finitely generated as an A-module, it follows that $M_{\mathfrak{m}}$ is finitely generated as an $A_{\mathfrak{m}}$-module. Since $A_{\mathfrak{m}}$ is a local ring, it has only one maximal ideal, namely $\mathrm{Jac}(A_{\mathfrak{m}}) = \mathfrak{m}$. Our hypothesis is that $\mathfrak{m}M_{\mathfrak{m}} = M_{\mathfrak{m}}$. Thus, by Nakayama's Lemma, we have $M_{\mathfrak{m}} = 0$. By part (i), $M = 0$.

Counter-example: Take $A = \mathbb{Z}$ and $M = \mathbb{Q}$. Note that $\mathbb{Q}$ is not a finitely-generated $\mathbb{Z}$-module. Note also that $\mathbb{Q}_{\mathfrak{m}} = \mathbb{Q}$ for all maximal ideals $\mathfrak{m} \subset \mathbb{Z}$, so $\mathbb{Q}_{\mathfrak{m}}/\mathfrak{m}\mathbb{Q}_{\mathfrak{m}} = 0$. Despite this, $\mathbb{Q} \neq 0$.

3. Let E/k be a finite-degree extension of fields.

(a) Prove that $\mathrm{Aut}(E/k)$ has at most $[E\colon k]$ elements.

Solution: Let $\mathrm{Aut}(E/k) = \{\sigma_1, \ldots, \sigma_m\}$ and $[E\colon k] = n$. We have to show that $m \leq n$.

Suppose for the sake of contradiction that $m > n$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a k-basis for E. Then the system

$$(*) \quad \begin{cases} \sigma_1(\alpha_1)x_1 + \ldots + \sigma_m(\alpha_1)x_m = 0 \\ \ldots \\ \sigma_1(\alpha_n)x_1 + \ldots + \sigma_m(\alpha_n)x_m = 0 \end{cases}$$

of n equations in m variables ($m > n$) must have a nontrivial solution $\beta_1, \ldots, \beta_m \in E$.

Let $c_1, \ldots, c_n \in k$ be arbitrary. Multiplying the ith equation of $(*)$ by c_i gives

$$\begin{cases} \sigma_1(c_1\alpha_1)\beta_1 + \ldots + \sigma_m(c_1\alpha_1)\beta_m = 0 \\ \ldots \\ \sigma_1(c_n\alpha_n)\beta_1 + \ldots + \sigma_m(c_n\alpha_n)\beta_m = 0 \end{cases}$$

Adding these equations, we observe that there exist $\beta_1, \ldots, \beta_n \in E$, not all zero, such that

$$\sigma_1\left(\sum_{i=1}^{n} c_i\alpha_i\right)\beta_1 + \ldots + \sigma_m\left(\sum_{i=1}^{n} c_i\alpha_i\right)\beta_m = 0 \quad \text{for all } c_1, \ldots, c_n \in k.$$

Since $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of E, this means that

$$\sigma_1(\omega)\beta_1 + \ldots + \sigma_m(\omega)\beta_n \quad \text{for all } \omega \in E.$$

But this implies that the distinct automorphisms $\sigma_1, \ldots, \sigma_m$ are k-linearly dependent, contradicting the linear independence of characters.

Remark: There is at least one other (completely different) way of solving this problem. If you know a simpler solution, please let me know and I'll include it (and credit you).

3. Let E/k be a finite-degree extension of fields.

(b) If E is a finite field, prove that $\mathrm{Aut}(E/k)$ is cyclic and the norm $E^\times \to k^\times$ is surjective.

Solution: Write $E = \mathbb{F}_{q^n}$, $k = \mathbb{F}_q$ and $[E\colon k] = n$, where q is a prime power. Then E is the splitting field of $x^{q^n} - x \in k[x]$, so that E/k is Galois, so $|\mathrm{Gal}(E/k)| = [E\colon k] = n$.

Since E is finite, the (injective) Frobenius endomorphism

$$\begin{aligned} \sigma\colon \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ \beta &\mapsto \beta^q \end{aligned}$$

is an automorphism over $\mathbb{F}_q$, so $\langle\sigma\rangle \leq \mathrm{Gal}(E/k)$. Since $\beta^{q^n} = \beta$ for all $\beta \in E$, we have $\sigma^n = \mathrm{Id}_E$. If we had $\sigma^i = \mathrm{Id}_E$ for some $i < n$, then $\beta^{q^i} = \beta$ for all $\beta \in E$, which is impossible since $x^{q^i} = x$ has only q^i roots. Thus, σ has order n, so $\mathrm{Gal}(E/k) = \langle\sigma\rangle$.

If $x \in E$, we have

$$N_{E/k}(x) = \prod_{\tau \in \mathrm{Gal}(E/k)} \tau(x) = x \cdot \sigma(x) \cdots \sigma^{n-1}(x) = x \cdot x^q \cdots x^{q^{n-1}} = x^\ell,$$

where we set

$$\ell = 1 + q + \ldots + q^{n-1} = \frac{q^n - 1}{q - 1}.$$

Since $E^\times$ is cyclic, we can write $E^\times = \langle\alpha\rangle$ for some $\alpha \in E$, so that $E = k(\alpha)$. Since $\ell q - \ell = q^n - 1$, we have $\alpha^{\ell q - \ell} = \alpha^{q^n - 1} = 1$, so $\alpha^{q\ell} = \alpha^\ell$. Thus, $(\alpha^{j\ell})^q = \alpha^{j\ell}$ for all $j \in \mathbb{N}$ and so $\alpha^{j\ell} \in \mathbb{F}_q$ for all $j \in \mathbb{N}$. Therefore,

$$k^\times = \mathbb{F}_q^\times = \{1, \alpha^\ell, \alpha^{2\ell}, \ldots, \alpha^{(q-2)\ell}\}.$$

Since $N_{E/k}(\alpha^j) = \alpha^{j\ell}$, it follows that $N_{E/k}\colon E^\times \to k^\times$ is surjective.

(Alternatively: Regard $N_{E/k}$ as a group homomorphism $E^\times \to k^\times$. Note that $\mathrm{Ker}(N_{E/k}) = \{x \in E^\times\colon x^\ell = 1\}$, so $|\mathrm{Ker}(N_{E/k})| \leq \ell$. Therefore,

$$|\mathrm{Im}(N_{E/k})| = \frac{|E^\times|}{|\mathrm{Ker}(N_{E/k})|} \geq \frac{q^n - 1}{\ell} = q - 1 = |k^\times|,$$

which shows that $N_{E/k}$ is surjective.)

(c) Give an example of a finite cyclic extension such that the norm is not surjective.

Example: $\mathbb{Q}(i)/\mathbb{Q}$. The Galois group is $\mathbb{Z}/2\mathbb{Z}$ and the norm is $N(a + bi) = a^2 + b^2$.

4. Let G be a finite group, F a field, and V a nonzero finite-dimensional F-linear representation of G.

(a) Give an example of G, F, and V such that V does not decompose as a direct sum of irreducible F-linear representations of G.

Example 1: Take $G = \mathbb{Z}/p\mathbb{Z} = \langle g \rangle$, $F = \mathbb{F}_p$. We claim that the regular representation of G over $\mathbb{F}_p$ does not decompose as a direct sum of irreducible representations. To see this, we show that every irreducible representation of G over $\mathbb{F}_p$ is trivial.

Let $\varphi\colon G \to \mathrm{GL}(V)$ be an irreducible representation. Since $\varphi(g)^p = \mathrm{Id}$, we see that the minimal polynomial $m \in \mathbb{F}_p[x]$ of $\varphi(g)$ has $m(x) \mid x^p - 1 = (x-1)^p$. In particular, 1 is an eigenvalue of $\varphi(g)$, so its eigenspace $E = \{v \in V\colon \varphi(g)v = v\}$ is a nonzero G-stable subspace. Since φ is irreducible, this implies that $E = V$, so $\varphi(g) = \mathrm{Id}_V$. This means that φ is the direct sum of $\dim(V)$ trivial representations. Again by the irreducibility of φ, it follows that $\dim(V) = 1$, so φ is trivial.

Therefore, since the regular representation of G over $\mathbb{F}_p$ is not the direct sum of trivial representations, it is not a direct sum of irreducible representations.

Example 2: Take $G = \mathbb{Z}/p\mathbb{Z} = \langle g \rangle$, $F = \mathbb{F}_p$. Let V be a 2-dimensional $\mathbb{F}_p$-vector space and fix a basis $\{e_1, e_2\}$. Define a representation $\varphi\colon G = \langle g \rangle \to \mathrm{GL}(V)$ via

$$\varphi(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Since $\varphi(g)$ is not diagonalizable, it follows that φ cannot decompose as a direct sum of two non-trivial G-invariant subspaces. Thus, the only possible decomposition of V as a direct sum of irreducible sub-representations is $V = V$, meaning that V is irreducible. But since V has a nontrivial proper G-invariant subspace (namely $\mathrm{span}\{e_1\}$), we see that V is not irreducible.

4. Let G be a finite group, F a field, and V a nonzero finite-dimensional F-linear representation of G.

(b) Suppose that the order of G is not zero in F. Prove that V is a direct sum of irreducible F-linear representations of G.

Solution: Let $\rho\colon G \to \mathrm{GL}(V)$ be a nonzero finite-dimensional F-linear representation of G. We proceed by induction on $\dim_F(V)$.

If V is irreducible, we're done. Assume, then, that V is reducible, so V has a nontrivial G-stable subspace $W \subset V$. Let W' be an F-vector space complement of W in V (which exists because $\dim_F(V) < \infty$), and let $\pi\colon V \twoheadrightarrow W$ denote the corresponding projection (i.e.: $\mathrm{Ker}(\pi) = W'$). Consider the averaged map

$$\begin{aligned} \pi^0 &\colon V \to V \\ \pi^0 &:= \frac{1}{|G|} \sum_{t \in G} \rho(t) \cdot \pi \cdot \rho(t)^{-1} \end{aligned}$$

Since $\pi\colon V \to W$ and $\rho(t)$ preserves W, we have $\pi^0\colon V \to W$. Moreover, since $x \in W$ implies $\rho(t)^{-1}x \in W$, we see that $x \in W$ implies $\rho(t) \cdot \pi \cdot \rho(t)^{-1}x = x$, which shows that $\pi^0|_W = \mathrm{Id}_W$. Thus, $\pi^0\colon V \to W$ is a projection map.

Let $W^0 := \mathrm{Ker}(\pi^0)$, so that $V = W \oplus W^0$ as F-vector spaces. We claim that W^0 is G-stable. To see this, note that for all $s \in G$

$$\rho(s) \cdot \pi^0 \cdot \rho(s)^{-1} = \frac{1}{|G|} \sum_{t \in G} \rho(s) \cdot \rho(t) \cdot \pi \cdot \rho(t)^{-1} \cdot \rho(s)^{-1} = \frac{1}{|G|} \sum_{t \in G} \rho(st) \cdot \pi \cdot \rho(st)^{-1} = \pi^0,$$

so that $\rho(s) \cdot \pi^0 = \pi^0 \cdot \rho(s)$. Thus, if $x \in W^0 = \mathrm{Ker}(\pi^0)$, then $\pi^0 \cdot \rho(s)x = \rho(s) \cdot \pi^0 x = 0$, so $\rho(s)x \in \mathrm{Ker}(\pi^0) = W^0$. Thus, W^0 is G-stable.

Therefore, $V = W \oplus W^0$ as representations. By induction hypothesis, both W and W^0 are direct sums of irreducible representations, so the same is true of V.

5. Let C_* be a complex of free abelian groups, with differential lowering the degree by 1. Let A be an abelian group.

(a) Construct a short exact sequence

$$0 \to H_n(C_*) \otimes_{\mathbb{Z}} A \to H_n(C_* \otimes_{\mathbb{Z}} A) \to \operatorname{Tor}_1^{\mathbb{Z}}(H_{n-1}(C_*), A) \to 0.$$

(Hint: use a short free abelian group resolution of A.)

Solution: Write $C_*\colon \cdots \to C_{n+1} \overset{d_{n+1}}{\to} C_n \overset{d_n}{\to} \cdots$. Let $Z_n := \operatorname{Ker}(d_n) \leq C_n$, $B_n := \operatorname{Im}(d_{n+1}) \leq C_n$. Note that both Z_n and B_n are free $\mathbb{Z}$-modules, and $H_n(C_*) = Z_n/B_n$.

Consider the short exact sequence $0 \to B_n \overset{\iota_n}{\hookrightarrow} Z_n \twoheadrightarrow H_n(C_*) \to 0$. Applying the long exact Tor sequence, and noting that Z_n is free (hence flat), we obtain an exact sequence

$$0 \to \operatorname{Tor}_1^{\mathbb{Z}}(H_n(C_*), A) \to B_n \otimes_{\mathbb{Z}} A \overset{\iota_n \otimes 1}{\to} Z_n \otimes A \to H_n(C_*) \otimes_{\mathbb{Z}} A \to 0.$$

From this, we observe that

$$\operatorname{Tor}_1^{\mathbb{Z}}(H_n(C_*), A) \cong \operatorname{Ker}(\iota_n \otimes 1), \tag{$*$}$$

$$H_n(C_*) \otimes_{\mathbb{Z}} A \cong \operatorname{Coker}(\iota_n \otimes 1). \tag{$**$}$$

Consider now the short exact sequence $0 \to Z_n \hookrightarrow C_n \overset{d_n}{\twoheadrightarrow} B_{n-1} \to 0$. Let $Z_* := \cdots \overset{0}{\to} Z_{n+1} \overset{0}{\to} Z_n \overset{0}{\to} \cdots$ denote the chain complex of Z_n's with differential 0. Define B_* similarly. By the long exact sequence on homology, we obtain an exact sequence

$$\cdots \to H_n(Z_* \otimes_{\mathbb{Z}} A) \overset{\varphi}{\to} H_n(C_* \otimes_{\mathbb{Z}} A) \overset{\psi}{\to} H_n(B_{*-1} \otimes_{\mathbb{Z}} A) \to \cdots$$

By our construction of Z_* and B_*, we have $H_n(Z_* \otimes_{\mathbb{Z}} A) \cong Z_n \otimes_{\mathbb{Z}} A$ and $H_n(B_{*-1} \otimes_{\mathbb{Z}} A) \cong B_{n-1} \otimes_{\mathbb{Z}} A$, thereby yielding

$$\cdots \overset{\iota_n \otimes 1}{\to} Z_n \otimes_{\mathbb{Z}} A \overset{\varphi}{\to} H_n(C_* \otimes_{\mathbb{Z}} A) \overset{\psi}{\to} B_{n-1} \otimes_{\mathbb{Z}} A \overset{\iota_{n-1} \otimes 1}{\to} \cdots$$

Breaking this long exact sequence into short exact sequences gives

$$0 \to \operatorname{Im}(\varphi) \hookrightarrow H_n(C_* \otimes_{\mathbb{Z}} A) \twoheadrightarrow \operatorname{Coker}(\varphi) \to 0.$$

We now note that

$$\operatorname{Im}(\varphi) \cong \frac{Z_n \otimes A}{\operatorname{Ker}(\varphi)} \cong \frac{Z_n \otimes A}{\operatorname{Im}(\iota_n \otimes 1)} \cong \operatorname{Coker}(\iota_n \otimes 1),$$

$$\operatorname{Coker}(\varphi) \cong \frac{H_n(C_* \otimes A)}{\operatorname{Im}(\varphi)} \cong \frac{H_n(C_* \otimes A)}{\operatorname{Ker}(\psi)} \cong \operatorname{Im}(\psi) \cong \operatorname{Ker}(\iota_{n-1} \otimes 1).$$

Thus, from the isomorphisms $(*)$, $(**)$, we thereby obtain the exact sequence

$$0 \to H_n(C_*) \otimes_{\mathbb{Z}} A \to H_n(C_* \otimes_{\mathbb{Z}} A) \to \operatorname{Tor}_1^{\mathbb{Z}}(H_{n-1}(C_*), A) \to 0.$$

5. Let C_* be a complex of free abelian groups, with differential lowering the degree by 1. Let A be an abelian group.

(b) Suppose that $H_n(C_*) = 0$ except for $n = 0$, and $H_0(C_*) \cong \mathbb{Z}_{(5)} \oplus \mathbb{Z}/5\mathbb{Z}$. Here, $\mathbb{Z}_{(5)}$ is the localization of $\mathbb{Z}$ at the prime (5). Compute the homology groups of $C_* \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$.

Solution: We claim that

$$H_n(C_* \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})) = \begin{cases} \mathbb{Z}_{(5)} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}/5\mathbb{Z} & \text{if } n = 1 \\ 0 & \text{else} \end{cases}$$

For each case, we will use the short exact sequence of (a):

$$0 \to H_n(C_*) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to H_n(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \to \mathrm{Tor}_1^{\mathbb{Z}}(H_{n-1}(C_*), \mathbb{Q}/\mathbb{Z}) \to 0. \qquad (*)$$

$\underline{n = 0}$: The short exact sequence $(*)$ reads:

$$0 \to \left(\mathbb{Z}_{(5)} \oplus \mathbb{Z}/5\mathbb{Z}\right) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to H_0(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \to 0 \to 0.$$

Thus,

$$\begin{aligned} H_0(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) &\cong (\mathbb{Z}_{(5)} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})) \\ &\cong \mathbb{Z}_{(5)} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}, \end{aligned}$$

where we have used the fact that $\mathbb{Z}/5\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

$\underline{n = 1}$: The short exact sequence $(*)$ reads:

$$0 \to 0 \to H_1(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \to \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}_{(5)} \oplus \mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to 0.$$

Thus, since $\mathbb{Z}_{(5)}$ is a flat $\mathbb{Z}$-module (by virtue of being a localization), we have

$$\begin{aligned} H_1(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) &\cong \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}_{(5)}, \mathbb{Q}/\mathbb{Z}) \oplus \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \\ &\cong \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}). \end{aligned}$$

To compute $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$, we apply the Tor long exact sequence to the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, obtaining

$$\mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}) \to \mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Z}/5\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Noting that $\mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}) = 0$ and $\mathbb{Z}/5\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, we have $\mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$.

(Alternatively: One can compute $\mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ by taking the projective resolution $0 \to \mathbb{Z} \xrightarrow{5} \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \to 0$ and applying $- \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$. One finds that $\mathrm{Tor}_1(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Ker}[\mathbb{Q}/\mathbb{Z} \xrightarrow{5} \mathbb{Q}/\mathbb{Z}] = \{0, 1/5, \ldots, 4/5\} \cong \mathbb{Z}/5\mathbb{Z}$.)

$\underline{n \neq 0, 1}$: The short exact sequence $(*)$ reads

$$0 \to 0 \to H_n(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \to 0 \to 0,$$

which gives $H_n(C_* \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) \cong 0$.

6. (a) State and prove Hilbert's Basis Theorem.

Statement: If A is a Noetherian ring, then $A[x]$ is a Noetherian ring.

Proof: Let $\mathfrak{a} \subset A[x]$ be an ideal. We will show that $\mathfrak{a}$ is finitely generated.

Let $I = \{c \in A\colon cx^n + (\text{lower terms}) \in \mathfrak{a}\} \subset A$ be the ideal of leading coefficients of the polynomials in $\mathfrak{a}$. Since A is Noetherian, I is finitely generated, say $I = (c_1, \ldots, c_n)$. Thus, for each $1 \leq i \leq n$, there is a polynomial $f_i \in \mathfrak{a}$ with $f_i(x) = c_i x^{r_i} + (\text{lower terms})$. Note that the polynomials f_i generate an ideal $(f_1, \ldots, f_n) \subset \mathfrak{a}$ in $A[x]$.

Let $r = \max\{r_1, \ldots, r_n\}$, where $r_i := \deg(f_i)$. We claim that every element $f \in \mathfrak{a}$ can be written

$$f = g + h,$$

where $g \in \mathfrak{a}$, $\deg(g) < r$ and $h \in (f_1, \ldots, f_r)$.

Proof of Claim: Let $f \in \mathfrak{a}$. Write $f = cx^m + (\text{lower})$. If $m < r$, we're done, so suppose $m \geq r$. Since $c \in I = (c_1, \ldots, c_n)$, we can write $c = u_1c_1 + \ldots + u_nc_n$, where $u_i \in A$, so that $f = (u_1c_1 + \ldots + u_nc_n)x^m + (\text{lower})$.

Note that $u_i x^{m-r_i} f_i = u_i c_i x^m + (\text{lower})$. Therefore, $f - \sum_{i=1}^n u_i x^{m-r_i} f_i \in \mathfrak{a}$ (since $f \in \mathfrak{a}$ and $f_i \in \mathfrak{a}$) and has degree $< m$. Continuing in this way, we can go on subtracting elements of $(f_1, \ldots, f_n)$ from f until we get a polynomial of degree $< r$, which we call g.

Let $M = A1 + Ax + \ldots + Ax^{r-1}$ be the A-module generated by $\{1, x, \ldots, x^{r-1}\}$. Then $f = g + h$ implies that

$$\mathfrak{a} = (\mathfrak{a} \cap M) + (f_1, \ldots, f_n).$$

Since A is Noetherian and M is a finitely-generated A-module, M is Noetherian. Therefore, $\mathfrak{a} \cap M \subset M$ is a finitely-generated A-submodule, so that $a \cap M = Ag_1 + \ldots + Ag_m$ for some $g_j \in M$. Thus, $\mathfrak{a} = (g_1, \ldots, g_m, f_1, \ldots, f_n)$, so $\mathfrak{a}$ is finitely generated.

(b) Let A be a Noetherian ring, and J an ideal of A. Define the ring $G_J(A) = A \oplus J \oplus J^2 \oplus \cdots$, in which the product of J^m and J^n is the usual product valued in the direct summand J^{n+m}. Prove that $G_J(A)$ is Noetherian.

Sketch: Since A is Noetherian, the ideal J is finitely generated, say $J = (r_1, \ldots, r_n)$. By Hilbert's Basis Theorem, $A[x_1, \ldots, x_n]$ is Noetherian. The idea now is to construct a surjective ring homomorphism

$$A[x_1, \ldots, x_n] \twoheadrightarrow G_J(A).$$

Doing so will show that $G_J(A)$ is Noetherian.

One such homomorphism can be constructed by decomposing polynomials in $A[x_1, \ldots, x_n]$ according to their degrees (that is, splitting polynomials into their homogeneous components) and evaluating at the point $(r_1, \ldots, r_n) \in A^n$.

8. Let $f\colon A \to B$ be a ring homomorphism.

(a) Define what it means to say that B is integral over A, and prove that this holds when B is finitely generated as an A-module.

Solution: We say that B is *integral over* A iff every $\beta \in B$ is integral over $f(A)$. That is, every $\beta \in B$ satisfies a monic polynomial with coefficients in $f(A)$.

Suppose B is a finitely-generated A-module, say $B = f(A)e_1 + \ldots + f(A)e_n$. Let $\beta \in B$. Write $\beta e_i = \sum_{j=1}^n a_{ij}e_j$ for $a_{ij} \in f(A)$, i.e. $\beta e_i - \sum_{j=1}^n a_{ij}e_j = 0$, so

$$\sum_{j=1}^{n} (\delta_{ij}\beta - a_{ij})e_j = 0, \qquad (*)$$

where δ_{ij} is the Kronecker delta.

Let $M = (\delta_{ij}\beta - a_{ij}) \in \mathrm{Mat}_n(f(A)[\beta])$. Multiplying $(*)$ by the adjugate $\mathrm{Adj}(M)$ gives

$$\det(M)e_i = 0 \quad \text{for each } e_i.$$

Since $1 \in B = f(A)e_1 + \ldots + f(A)e_n$, it follows that $\det(M)\cdot 1 = 0$, i.e.: $\det(\delta_{ij}\beta - a_{ij}) = 0$ in $f(A)[\beta]$. That is, β satisfies a monic polynomial with coefficients in $f(A)$.

(b) If B is finitely generated as an A-module, prove that $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a closed map. (Hint: reduce to the case where f is injective.)

Solution:

9. Let p be an odd prime. In this question, ζ_p denotes a primitive pth root of unity.

(a) Describe $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and determine all primes p such that $\mathbb{Q}(\zeta_p)$ contains a subfield L whose Galois group over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Solution: Consider the homomorphism

$$\begin{aligned} \psi\colon (\mathbb{Z}/p\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ a \pmod p &\mapsto \sigma_a\colon [\zeta_p \mapsto \zeta_p^a] \end{aligned}$$

Note that ψ is injective. Since $|\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = [\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = \varphi(p) = p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$, we see that ψ is an isomorphism. Thus, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Note that if $\mathbb{Q}(\zeta_p)$ contains a subfield L with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, then $5 = [L\colon \mathbb{Q}] \mid [\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p-1$, so $p \equiv 1 \pmod 5$.

Conversely, suppose $p \equiv 1 \pmod 5$. Then $5 \mid p-1$, so $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ contains a subgroup H of order $|H| = \frac{p-1}{5}$. Let $L = \mathbb{Q}(\zeta_p)^H$. Then

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/L)} \cong \frac{\mathbb{Z}/(p-1)\mathbb{Z}}{H} \cong \mathbb{Z}/5\mathbb{Z}.$$

(b) Prove that there is a finite Galois extension E of $\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ by constructing E as a subfield of an explicit Galois extension $F/\mathbb{Q}$, and explicitly describe the subgroup $\mathrm{Gal}(F/E) \subset \mathrm{Gal}(F/\mathbb{Q})$.

Solution: Let $F = \mathbb{Q}(\zeta_{341})$, noting that $341 = 11 \cdot 31$. Note that

$$\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/341\mathbb{Z})^\times \cong (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/31\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

Let $H_1 \leq \mathbb{Z}/10\mathbb{Z}$ have $|H_1| = 2$. Let $H_2 \leq \mathbb{Z}/30\mathbb{Z}$ have $|H_2| = 6$. By the above isomorphisms, we can regard $H_1 \times H_2 \leq \mathrm{Gal}(F/\mathbb{Q})$.

Let $E = F^{H_1 \times H_2}$. Then

$$\mathrm{Gal}(F/E) \cong H_1 \times H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

and

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \frac{\mathrm{Gal}(F/\mathbb{Q})}{\mathrm{Gal}(F/E)} \cong \frac{\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}}{H_1 \times H_2} \cong \frac{\mathbb{Z}/10\mathbb{Z}}{H_1} \times \frac{\mathbb{Z}/30\mathbb{Z}}{H_2} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

10. (a) Let G be a group and H a subgroup of finite index $n > 0$. Prove that G contains a normal subgroup of index at most $n!$. (Hint: think about homomorphisms from G to S_n.)

Solution: Consider the action of G on the set G/H by left multiplication. Let π denote the permutation representation of the action, i.e.,

$$\begin{aligned} \pi\colon G &\to \mathrm{Perm}(G/H) \cong S_n \\ g &\mapsto [g'H \mapsto gg'H]. \end{aligned}$$

Let $N := \mathrm{Ker}(\pi)$, so $N \trianglelefteq G$ and

$$|G\colon N| = |G/\mathrm{Ker}(\pi)| = |\mathrm{Im}(\pi)| \leq |\mathrm{Perm}(G/H)| = n!$$

(b) Let G be a group which is generated by two elements. Prove that G has at most 17 subgroups of index 3. (Hint: think about homomorphisms from G to S_3.)

Sketch: Every index-3 subgroup determines two homomorphisms $\varphi\colon G \to S_3$ in which $\varphi(G)$ acts transitively on $\{1,2,3\}$. Conversely, every homomorphism $\varphi\colon G \to S_3$ in which $\varphi(G)$ acts transitively on $\{1,2,3\}$ determines one index-3 subgroup of G. Thus, we have

$$\#\text{ index 3 subgroups of } G = \frac{1}{2}\,\#\{\varphi\colon G \to S_3\colon \varphi(G) \text{ acts transitively on } \{1,2,3\}\}.$$

Since G is generated by 2 elements,

$$\#\{\varphi\colon G \to S_3\colon \varphi(G) \text{ acts transitively on } \{1,2,3\}\} \leq |\mathrm{Hom}(\mathrm{Free}(2), S_3)| - 1,$$

where $\mathrm{Free}(2)$ denotes the free group on 2 generators. Since $|\mathrm{Hom}(\mathrm{Free}(2), S_3)| = (3!)^2 = 36$, we conclude that

$$\#\text{ index 3 subgroups of } G \leq \frac{1}{2}(36-1) = 17.5.$$