

EXAMPLE-BASED EXERCISES IN ALGEBRA

XU RUICHEN

ABSTRACT. This note is a reorganized summary prepared by the author during the second phase of the doctoral qualification exam in algebra in Fall 2022. The exam covered the following topics:

- Galois theory,
- module theory,
- representation theory of finite groups,
- homological algebra.

The purpose of this compilation is to explore various examples and thereby develop a deeper understanding of these subjects. We warmly welcome comments and supplementary examples that may enrich the material.

At present, the solutions to the exercises have not been included due to time constraints. Moreover, we should also include some theoretic examples. In the future, we hope to provide solutions together with guiding remarks to make the collection more complete.

Although working through various examples is both challenging and rewarding, one should avoid becoming overly absorbed in them; it is important to move on to more advanced topics in a timely manner.

CONTENTS

1. Galois theory	1
2. Representation theory of finite groups	3
3. Homological algebra	5

1. GALOIS THEORY

1.1. Galois group of polynomials.

1.1.1. *Compute the Galois group of polynomials, and try to draw the subfield and subgroup lattices. Do not forget to check the irreducibility of these polynomials if so.*

- (1) $P(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$,
- (2) $P(X) = X^3 - 3X - 3 \in \mathbb{Q}[X]$,
- (3) $P(X) = (X^2 - 2)(X^2 - 8) \in \mathbb{Q}[X]$,
- (4) $P(X) = (X^2 + 1)(X^2 - 2) \in \mathbb{Q}[X]$,
- (5) $P(X) = X^4 + X^2 + 4 \in \mathbb{Q}[X]$,
- (6) $P(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$,
- (7) $P(X) = X^4 + 3X^2 + 3 \in \mathbb{Q}[X]$,
- (8) $P(X) = X^4 + 8X + 12 \in \mathbb{Q}[X]$,
- (9) $P(X) = X^4 - 2X + 2 \in \mathbb{Q}[X]$,
- (10) Systematically discuss $P(X) = X^4 + pX + p \in \mathbb{Q}[X]$ when p is a prime,
- (11) $P(X) = X^4 + 8X + 12 \in F[X]$ for any quadratic extension F over \mathbb{Q} .
- (12) $P(X) = X^3 - X - 1 \in \mathbb{Q}(\sqrt{-23})[X]$,
- (13) $P(X) = X^3 - 3X - 1 \in F[X]$ for any quadratic extension F over \mathbb{Q} .
- (14) $P(X) = X^4 - 2 \in \mathbb{Q}(\sqrt{-1})[X]$,

- (15) $P(X) = X^4 - 4X^1 + 5 \in \mathbb{Q}(\sqrt{5})[X]$,
 (16) $P(X) = X^4 - 4X + 5 \in \mathbb{Q}(\sqrt{5})[X]$.

1.1.2. Modulo- p method.

- (1) (The criterion for $G = \mathfrak{S}_p$ or not on the degree p polynomials) $P(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$.
 (2) $P(X) = X^6 + 22X^5 + 21X^4 + 13X^3 - 37X^2 - 29X - 15 \in \mathbb{Q}[X]$,
 (3) $P(X) = X^4 + 5X^3 - 2X^2 - 1 \in \mathbb{Q}[X]$.

1.1.3. *Two extra examples.* For field F which is not of characteristic 2 (if it simplifies the computation).

- (1) $P(X) = X^3 + uX + u \in F(u)[X]$,
 (2) $P(X) = X^4 + uX + u \in F(u)[X]$.

1.2. Determine intermediate fields.

1.2.1. *Please determine all the intermediate fields and draw the subfield and subgroup lattices as explicit as possible. Do not forget to try to explicitly write the elements in Galois groups.*

- (1) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$,
 (2) $\mathbb{Q}(\sqrt{2}, \sqrt{-1})/\mathbb{Q}$, and convince yourself that this is $\mathbb{Q}(\zeta_8)$,
 (3) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ and its Galois closure. Try to compute $\mathbb{Q}(\sqrt[4]{2}, \zeta_8)/\mathbb{Q}$ directly.
 (4) the splitting field of $X^8 - 2$ over \mathbb{Q} (observe the pattern of $X^2 - 2$, $X^4 - 2$ and $X^8 - 2$, can we generalize it to $X^{2^m} - 2$ over \mathbb{Q} ?).
 (5) the splitting field of $X^8 - 3$ over \mathbb{Q} (compare it with that of $X^8 - 2$ over \mathbb{Q}),
 (6) the splitting field of $X^p - 2$ over \mathbb{Q} , for p a prime number.
 (7) the splitting field of $X^4 - X^2 - 1$ over \mathbb{Q} ,
 (8) the splitting field of the minimal polynomial of $\sqrt[3]{2} + \sqrt{3}$ over \mathbb{Q} .

1.2.2. *Compute the automorphism groups of the following non-Galois extensions.*

- (1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$,
 (2) $X^n - u \in F(u)[X]$,
 (3) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$: there is no \mathbb{Q} -automorphism sending $\sqrt{2}$ to $-\sqrt{2}$.

1.2.3. *Try to find a primitive element of the field extensions.*

- (1) $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})/\mathbb{Q}$, check: $\sqrt[4]{2} + \sqrt{-1}$ works.
 (2) $\mathbb{Q}(\zeta_{37})$, check: $\zeta_{37} + \zeta_{37}^{10} + \zeta_{37}^{26}$ works (is there a theoretical reason why this works?).
 (3) For the splitting field of the minimal polynomial of $\alpha := \sqrt[3]{2} + \sqrt{3}$ over \mathbb{Q} , check: $\alpha + \sqrt{-1}$ works.

1.2.4. *Fundamental theorem of symmetric polynomials.* Let F be a field, and T_1, \dots, T_n are indeterminates over F . Consider for $1 \leq k \leq n$ the polynomials

$$S_k(T_1, \dots, T_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} T_{i_1} \cdots T_{i_k}.$$

Consider $L = F(T_1, \dots, T_n)$ and $K = F(S_1, \dots, S_n)$.

- (1) Prove that $K = L^{\mathfrak{S}_n}$, hence proving the fundamental theorem of symmetric polynomials.
 (2) Prove that $T_1 T_2^2 \cdots T_n^n$ is a primitive element for the extension L/K .

1.3. Finite fields.

1.3.1. *An interesting problem.*

- (1) Let u be algebraic over \mathbb{F}_p and $F := \mathbb{F}_p(u)$. Is u necessarily a generator of F^\times ?

1.3.2. Check the irreducibility of the following polynomials.

- (1) $P(X) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$,
- (2) $P(X) = X^3 - 2 \in \mathbb{F}_7[X]$,

1.3.3. Let K be the splitting field of $P(X)$, compute $[K : \mathbb{F}_p]$.

- (1) $P(X) = X^4 + 1 \in \mathbb{F}_p[X]$ for any prime p ,
- (2) $P(X) = X^4 - 2(p_1 + p_2)X^2 + (p_1 - p_2)^2 \in \mathbb{F}_p[X]$ for any two distinct primes p_1 and p_2 .

These are two examples of polynomials that are irreducible over \mathbb{Q} but are reducible over any finite field \mathbb{F}_p .

1.3.4. Compute the subgroup and subfield lattice of $\mathbb{F}_{p^{12}}/\mathbb{F}_p$.

1.3.5. Consider the $Q(X) = X^q - X - a \in \mathbb{F}_{q^n}[X]$.

- (1) Let α be a root of $Q(X)$ in $\overline{\mathbb{F}_{q^n}}$, prove that $\alpha^{q^n} = \alpha + \text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a)$, and find $[\mathbb{F}_{q^n}(\alpha) : \mathbb{F}_{q^n}]$,
- (2) Assume $n = 1$ and $a \in \mathbb{F}_q^\times$, decompose $Q(X)$ into irreducibles in $\mathbb{F}_q[X]$.

1.4. Cyclotomic Fields.

1.4.1. Determine the Galois group. Let K be a field, it is known that $\text{Gal}(K(\zeta_n)/K)$ embeds into $(\mathbb{Z}/n\mathbb{Z})^\times$. What is its image?

- (1) $K = \mathbb{Q}$,
- (2) $K = \mathbb{R}$,
- (3) $K = \mathbb{F}_p$. For example, compute $[\mathbb{F}_p(\zeta_7) : \mathbb{F}_p]$. This shows all subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ are possible to appear.

1.4.2. Composition and intersections. Suppose $\text{char } F \nmid m, n$.

- (1) prove or disprove that $K(\zeta_m)K(\zeta_n) = K(\zeta_{[m,n]})$,
- (2) prove or disprove that $K(\zeta_m) \cap K(\zeta_n) = K(\zeta_{(m,n)})$,

1.4.3. Intermediate fields.

- (1) For $n > 2$, prove that $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the maximal real subfield of index 2,
- (2) Determine all quadratic subfields of $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ for primes p (odd and even) and $n \geq 1$.

There is a general framework. Let E be a field containing all n -th root of unity. Let $\mu_n^\circ(E)$ be the set of all primitive n -th root of unity.

- (3a) Prove that $\sum_{\zeta \in \mu_n^\circ(E)} \zeta = \mu(n)$, and compute $\prod_{\zeta \in \mu_n^\circ(E)} \zeta$. Here $\mu(n)$ is the Mobius function.
- (3b) Let F be a field with $E = F(\zeta_n)$, such that $[E : F] = \varphi(n)$, prove that $\mu_n^\circ(E)$ is F -linearly independent if and only if n is square-free. Moreover when n is square-free, for any $H \leq \text{Gal}(E/F)$, prove that $E^H = \sum_{\sigma \in H} \sigma(\zeta_n)$.
- (4) Use these results, try to draw the subgroup and subfield lattice of $\mathbb{Q}(\zeta_n)$ for n at least up to 15.

2. REPRESENTATION THEORY OF FINITE GROUPS

2.1. Permutation groups.

- (1) Write the conjugacy classes of \mathfrak{S}_n , the number of elements in each conjugacy classes.
- (2) (From \mathfrak{S}_n to \mathfrak{A}_n) Passing to \mathfrak{A}_n , which of these conjugacy classes will split. Given a representation V_λ of \mathfrak{S}_n with respect to the Young diagram λ , describe the structure of $\text{Res}_{\mathfrak{A}_n}^{\mathfrak{S}_n} V_\lambda$. Let W_λ be a subquotient of $\text{Res}_{\mathfrak{A}_n}^{\mathfrak{S}_n} V_\lambda$, describe the structure of $\text{Ind}_{\mathfrak{A}_n}^{\mathfrak{S}_n} W_\lambda$. Describe the characters of these representations.
- (3) (sign representation) Prove that V_{λ_1} is isomorphic to $V_\lambda \otimes \text{sgn}$ where sgn is the sign representation of \mathfrak{S}_n . Draw their Young diagrams. Prove that $\text{Ind}_{\mathfrak{A}_n}^{\mathfrak{S}_n}$ is isomorphic to $\mathbf{1} \oplus \text{sgn}$.

- (4) (From \mathfrak{S}_n to \mathfrak{S}_{n+1}) Describe the branching law.
- (5) (standard representations) Let F^n be the permutation representation of \mathfrak{S}_n , and define the *standard representation* std as the kernel of $F^n \rightarrow 1$. Prove that std is an irreducible representation of \mathfrak{S}_n , and draw its Young diagram. More generally, prove that for $0 \leq k \leq n-1$, the exterior product $\wedge^k \text{std}$ is an irreducible representation of \mathfrak{S}_n .
- (6) Draw the character table of \mathfrak{S}_n and \mathfrak{A}_n for $n = 3, 4, 5$ and recognize each irreducible representations.

2.2. Groups by presentations. Draw the character tables and try to recognize each irreducible representations.

- (1) (Cyclic groups) Cyclic groups of order n ,
- (2) (Dihedral groups) $\text{Dih}_n := \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle$,
- (3) $Q = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b \rangle$ (a group of order 8),
- (4) $T = \langle a, b \mid a^3 = b^4 = 1, bab^{-1} = a^2 \rangle$. Good new: up to now, we are managed to compute the character table of all nonabelian groups of order ≤ 15 .
- (5) (Dicyclic groups) $\text{Dic}_n = \langle a, b \mid a^{2n} = 1, b^2 = a^n, b^{-1}ab = a^{-1} \rangle$. Note that Dic_1 is the cyclic group of order 4, Dic_2 is the group Q in question (2), and Dic_3 is the group T in question (3).
- (6) $S = \langle a, b \mid a^8 = b^2 = 1, bab^{-1} = a^3 \rangle$ (a group of order 16). Note that this is the Galois group of $X^8 - 2 \in \mathbb{Q}[X]$ as we have computed previously (although expressed in different generators).
- (7) (semidihedral groups) $\text{SDih}_n = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, bab^{-1} = a^{2^{n-2}-1} \rangle$. Note that SDih_4 is the group S in question (5).

2.3. Matrix groups. Draw the character tables and try to recognize each irreducible representations. Here suppose $p > 2$ is a prime and $q = p^n$ for some integer $n \geq 1$.

- (1) $\text{GL}_2(\mathbb{F}_q)$,
- (2) $\text{SL}_2(\mathbb{F}_q)$,
- (3) The affine group

$$\text{Aff}_2(\mathbb{F}_p) := \{ \phi : \mathbb{F}_p \rightarrow \mathbb{F}_p \mid x \mapsto ax + b, a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \} = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}.$$

Note that this is the Galois group of $X^p - 2 \in \mathbb{Q}[X]$. By reading the character table (see later exercises), one shows that this polynomial is solvable (even if p can be larger than 5).

- (4) Upper triangular matrices $\text{B}_2(\mathbb{F}_q)$.

2.4. Information from character tables. Let $\varphi : G \rightarrow \text{GL}_2(\mathbb{C})$ be a representation and χ be its character. Let $\varphi_1, \dots, \varphi_r$ be all irreducible representations of G , with characters χ_1, \dots, χ_r accordingly.

- (1) (Order of the group) How to read the order of G from its character table.
- (2) (Read $\ker \varphi$) Prove that $\ker \varphi = \{g \in G : \chi(g) = \chi(1)\}$. This can be used to judge if a representation is faithful or not.
- (3) (Determine all normal subgroups of G) Let N be a normal subgroup of G and $\varphi_1, \dots, \varphi_r$ be all irreducible representations of G , prove that N is the intersection of some $\ker \varphi_i$, and these exhaust all normal subgroups of G .
- (4) (Determine the commutator of G) Prove that $[G, G]$ is the intersection of kernels of all one dimensional irreducible representations of G .
- (5) (Determine the center of G) Use the second orthogonality to calculate the number of elements in each conjugacy class of G . Then $Z(G)$ is the union of conjugacy classes with only one element.

- (6) (Passing to the quotient) Let N be a normal subgroup of G and let $\varphi_1, \dots, \varphi_s$ be those such that $N \subseteq \ker \varphi_i$. Then $\varphi_1(\text{mod } N), \dots, \varphi_s(\text{mod } N)$ are all irreducible representations of G/N . Let $\{g_1, \dots, g_t\}$ be a set of representatives of conjugacy classes of G . Then $g_j N$ is conjugate to $g_\ell N$ if and only if $\chi_i(g_j) = \chi_i(g_\ell)$ for any $i = 1, \dots, s$. These results shall be enough to draw the character table for G/N .

We have so far computed character tables for so many groups. So you can consider the questions (1) to (5) above for these groups. For (5), it might be interesting to consider $N = Z(G)$ so as to use the information in question (4). For some particular groups, with these informations, you can try to compute all Sylow p -subgroups, or determine whether it is solvable, simple, etc.

3. HOMOLOGICAL ALGEBRA

3.1. Calculating the Tor functor. Let R be a ring and B be an R -module, and I, J be ideals of R . Let k be a field.

- (1) $\text{Tor}_i^{\mathbb{Z}}(A, B)$ for $A, B \in \{\mathbb{Z}/m, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}/\mathbb{Z}\}$,
- (2) Let R be a ring and a be a nonzerodivisor in R , (try to) compute $\text{Tor}_i^R(A, B)$ for $A, B \in \{R/a, R\}$,
- (3) Let R be a ring and $a \in R$, possibly a zerodivisor in R . For any R -module B , prove that there exists an exact sequence

$$0 \rightarrow \text{Tor}_2^R(R/aR, B) \rightarrow R[a] \otimes_R B \rightarrow B[a] \rightarrow \text{Tor}_1^R(R/aR, B) \rightarrow 0.$$

We remark that this is not easy and a possible short path is to invoke theories in derived categories.

- (4) $\text{Tor}_1^R(R/I, R/J)$,
- (5) Let $R = k[X, Y]$, $I = (X, Y)$. Prove that $\text{Tor}_1^R(I, k) \cong \text{Tor}_2^R(k, k) = k$. In general, compute $\text{Tor}_i^R(B, k)$.
- (6) Let $R = \mathbb{Z}[X]$, and \mathbb{Z} is an R -module via $X \mapsto 0$. Compute $\text{Tor}_i^R(\mathbb{Z}, \mathbb{Z})$.
- (7) Let $R = \mathbb{Z}/m$ and $A = \mathbb{Z}/d$, with $d \mid m$, which is an R -module via the natural map $\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/d$. Compute $\text{Tor}_i^R(\mathbb{Z}/d, B)$.
- (8) Let R be a UFD with $a, b \in R$ coprime. Compute $\text{Tor}_i^{R/(ab)}(R/a, R/b)$.
- (9) Let $R = \mathbb{Z}[\zeta_m]$ for $m \geq 3$. Compute $\text{Tor}_i^R(\mathbb{Z}, B)$.
- (10) Let $R = k[X]/(X^m)$ for $m \geq 2$. Compute $\text{Tor}_i^R(k, B)$, and more generally $\text{Tor}_i^R((X^k), B)$ for $k < m$.
- (11) Let R be a domain, $Q := \text{Frac}(R)$ and V be a Q -vector space, regarded as an R -module. Assume that B has a nonzero annihilator. Compute $\text{Tor}_i^R(V, B)$.
- (12) Let $R = k[X, Y, Z, W]/(XW - YZ)$, and regard k as an R -module via the quotient map sending X, Y, Z, W to 0. Compute $\text{Tor}_i^R(k, R/(X))$ and $\text{Tor}_i^R(k, R/(X, Y))$.

3.2. Calculating the Ext functor.

- (1) Consider the parallel questions (1) - (11) in the previous section for Ext.
- (2) (A vanishing result) Prove that $\text{Ext}_{\mathbb{Z}}^i(A, B) = 0$ for any $i \geq 2$.
- (3) Let $R = \mathbb{Z}/m$ and $A = \mathbb{Z}/d$, with $d \mid m$, which is an R -module via the natural map $\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/d$. Compute $\text{Ext}_R^i(\mathbb{Z}/d, B)$, $\text{Ext}_R^i(B, \mathbb{Z}/d)$, and when $d^2 \mid m$, compute $\text{Ext}_R^i(\mathbb{Z}/d, \mathbb{Z}/d)$.

3.3. Group cohomology. Let G be a group and A be a $\mathbb{Z}[G]$ -module.

3.3.1. Compute $H_i(G, A)$ and $H^i(G, A)$.

- (1) Allowing G to be any group and $A := \mathbb{Z}[G]$ be the regular $\mathbb{Z}[G]$ -module.
- (2) (Trivial coefficient) Let A be a trivial G -module. Prove that $H_0(G, A) = A$, $H_1(G, A) = G^{\text{ab}} \otimes_{\mathbb{Z}} A$. Prove that $H_0(G, A) = A$, $H_1(G, A) = \text{Hom}_{\text{Grp}}(G, A)$. What can we say for higher (co)homology?

- (3) (Cyclic group) Let $G := C_m$ be the cyclic group of order m .
- (4) (Infinite cyclic group) Let $G := C_\infty$ be the infinite cyclic group (isomorphic to \mathbb{Z}).
- (5) (Free group) Let G be a free group over a set X . In particular, consider the case when $|X| = 1, 2$.
- (6) (Dihedral groups) Let $G = \text{Dih}_m := C_m \rtimes C_2$ where m is an odd integer, and $A = \mathbb{Z}$ be a trivial $\mathbb{Z}[G]$ -module. One can try to use Hochschild-Serre spectral sequence with $H = C_m$ and $G/H = C_2$. Why the case when m is even is more challenging?
- (7) (Infinite dihedral groups) Let $G = \text{Dih}_\infty := C_\infty \rtimes C_2$.
- (8) (Product of cyclic groups) Let $G = C_m \times C_m$ and $A = \mathbb{Z}$ be a trivial $\mathbb{Z}[G]$ -module.
- (9) (Hopf theorem) Let G be given as a quotient of a free group F by a subgroup of relations R . Prove that $H^2(G, \mathbb{Z}) = (R \cap [F, F])/[F, R]$.

3.3.2. *A dévissage.* Let $R \rightarrow S$ be a ring homomorphism, A and B are R -modules.

- (1) Let R be a left noetherian ring, A be a finitely generated R -module, I is an injective R -module. Prove that there is a natural bijection

$$\text{Tor}_n^R(\text{Hom}_S(B, I), A) \xrightarrow{\sim} \text{Hom}_S(\text{Ext}_R^n(A, B), I).$$

- (2) Take $R = \mathbb{Z}[G]$, $S = \mathbb{Z}$, $I = \mathbb{Q}/\mathbb{Z}$, $A = \mathbb{Z}$, what can we get?

3.4. Spectral sequences.

3.4.1. *Review: what can we say on H^n ?*

- (1) Spectral sequences collapsing on either p -axis or q -axis.
- (2) Spectral sequences with only two nonzero rows and columns.
- (3) Five term exact sequence.
- (4) How to prove the universal coefficient theorem using spectral sequences. What about Kunneth's theorem?

3.4.2. *Review: How to construct spectral sequences.*

- (1) Grothendieck's spectral sequence.
- (2) Spectral sequence involving Tor and Ext,
- (3) Hochschild-Serre spectral sequence,
- (4) (*) Leray spectral sequence.

3.5. Derived categories.

- (1) Let \mathcal{A} be an abelian category. When is $\mathbf{D}(\mathcal{A})$ an abelian category. [Answer: If and only if \mathcal{A} is a split abelian category.] Given examples when $\mathbf{D}(\mathcal{A})$ is (is not) an abelian category.
- (2) (Understand the morphisms in derived categories) Do Weibel Exercise 10.4.2. In particular, give examples:
 - (a) A morphism $g : X \rightarrow Y$ in $\mathbf{C}(\mathcal{A})$ such that g induces zero maps on cohomology, but $g \neq 0$ in $\mathbf{D}(\mathcal{A})$.
 - (b) A morphism f is zero in $\mathbf{D}(\mathcal{A})$ but not nullhomotopic.
- (3) (Dévissage and derive) Do Weibel Exercise 10.8.3 and Exercise 10.8.4.
- (4) There are some interesting exercises in Kashiwara-Shapiro: Exercise 13.1, 13.2, 13.3, 13.4.

ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE, CHINESE ACADEMY OF SCIENCES, NO. 55 ZHONG-GUANCUN EAST ROAD, BEIJING, 100190, CHINA.

Email address: xuruichen21@mails.ucas.ac.cn