Algebra: Practice Problems

These problems are intended for you to work on to help you review the material. Several of the practice problems are longer problems than what you will find on the exam, whereas some are much more basic. Do as many as you can. Bring your questions on incompleted problems to the afternoon sessions, and bring your solutions to completed problems to present also in the afternoon sessions.

1 Groups

1. Prove that the additive group of real numbers $(\mathbb{R}, +)$ is isomorphic to the multiplicative group $(\mathbb{R}^{>0}, .)$ of positive reals.

2. Let $(G, \cdot)$ be a group. Define G^{op} to be the group whose underlying set of points is G but with multiplication operation $*$ defined by :

$$a * b := b \cdot a$$

   Prove that $(G^{op}, *)$ is a group and construct a group isomorphism $\phi : G \to G^{op}$.

3. Determine the number of elements in $\operatorname{Aut} G$, the automorphism group of G for the following groups :

   (a) C_{12}

   (b) D_8

4. If G is a group which has a unique element x of order k (k is some positive integer), then show that $k = 2$ and $x \in Z(G)$ (the center)

5. Let H, N be subgroups of G with N normal. Show that the set $HN := \{hn : h \in H, n \in N\}$ is a subgroup of G.

6. If $G/Z(G)$ is cyclic, show that G is abelian.

Group actions, class equation etc

7. Let H be a subgroup of G and let

$$K := \bigcap_{a \in G} aHa^{-1}$$

   (K is the largest normal subgroup of G which is contained in H). Prove that the index $|H : K|$ divides $(|G : H| - 1)!$

8. If $|G| = p^n$ for some prime p and integer $n \geq 1$, show that $\{1\} \subsetneq Z(G)$. Using this or otherwise, show that a group of order p^2 (p prime) must be abelian.

Sylow theorems

9. If $|G| = pq$ with p, q distinct primes, show that G is not simple.

2 Rings

Note: 'Ring' will always mean a ring with identity.

1. Let I be the ideal of the polynomial ring $\mathbb{R}[x]$ generated by x^2+2x+3. Prove that the quotient ring $\mathbb{R}[x]/I$ is isomorphic (as rings) to $\mathbb{C}$.

2. Let R be an integral domain and $R[[x]]$ be the ring of formal power series in the indeterminate x with coefficients in R. Show that the ideal (x) in $R[[x]]$ is prime. Also prove that: (x) is maximal $\iff$ R is a field.

3. Suppose R is a commutative ring and for each $a \in R$, there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal in R is maximal.

4. Let R be a Euclidean domain with norm function $N(\cdot)$. Let $m := \min\{N(x) : x \neq 0\}$. Prove that any $y \neq 0$ with $N(y) = m$ must be a unit in R.

5. If R is a P.I.D, and $a, b \in R$ such that $(a) + (b) = R$, show that $gcd(a, b) = 1$.

6. If R is a P.I.D and P is a prime ideal in R, then is R/P necessarily a P.I.D ?

7. If R is a P.I.D, then show that the ascending chain condition on ideals holds i.e, given ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in R, there exists N such that $I_j = I_{j+1}$ for all $j \geq N$.

3 Problems on Fields, Galois theory

1. Prove that the following statements are equivalent for a quadratic $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$.

(a) $f(x)$ is irreducible over $\mathbb{Q}$

(b) $\sqrt{b^2-4ac} \notin Q$

(c) $\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2-4ac}/Q)$ has order 2.

2. Let $f(x) \in E[x]$, where E is a field, and let $\sigma : E \to E$ be an automorphism. If f splits and σ fixes every root of f, prove that σ fixes every coefficient of $f(x)$. What if σ just preserves the set of roots?

3. Determine the irreducible polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.

4. Let α denote the positive real fourth root of 2. Factor the polynomial $x^4 - 2$ into irreducible factors over each of the following fields: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha, i)$.

5. Let K/F be a finite extension. Prove that $\mathrm{Aut}_F(K)$ is a finite group.

6. Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F?

7. Let $\zeta = e^{2\pi i/3} \in \mathbb{C}$ be a cube root of 1. Let $\alpha = \sqrt[3]{a + b\sqrt{2}}$, and let K be the splitting field of the irreducible polynomial for α over $\mathbb{Q}$. Determine the possible Galois groups of K over $\mathbb{Q}(\zeta)$.

8. Determine the degree of a primitive 7th root of unity ζ over $\mathbb{Q}(\omega)$, where ω is a primitive 3rd root of unity.

9. Determine the Galois groups of the polynomials $x^8 - 1$, $x^{12} - 1$, $x^9 - 1$.

10. Prove that $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ is a cyclic group of order r, generated by the Frobenius map ϕ. ($\phi(x) = x^p$.)

11. Let ϕ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Determine the rational canonical form for ϕ considered as an $\mathbb{F}_p$-linear transformation of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$. (As a bonus question, compute the Jordan canonical form (over a field containing all the eigenvalues).)

12. Determine the degree of the splitting field for the following polynomials over $\mathbb{Q}$. (a) $x^4 - 1$ (b) $x^3 - 2$ (c) $x^4 + 1$

13. Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$.

14. Let $K \supset L \supset F$ be fields. Prove or disprove:

(a) If K/F is Galois, then K/L is Galois.

(b) If K/F is Galois, then L/F is Galois.

(c) If L/F and K/L are both Galois, then K/F is Galois.

15. Let $\mathbb{F}$ be a field, and let R be the set of 2×2 matrices of the form

$$\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{F}\}.$$

Show that with the usual matrix operations, R is a commutative ring with identity. For which of the following fields $\mathbb{F}$ is R a field: $\mathbb{F} = \mathbb{Q}, \mathbb{C}, \mathbb{F}_5, \mathbb{F}_7$?

16. Let $F \subset K$ be fields and $a, b \in K$ be algebraic over F. Show $a + b$ is algebraic over F.

17. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$. Prove that K is a Galois extension of $\mathbb{Q}$ and determine its Galois group.

18. Let p be an odd prime. How many elements of $\mathbb{F}_p$ have square roots in $\mathbb{F}_p$? How many have cube roots in $\mathbb{F}_p$?

19. Let $f \in F[x]$ be a separable polynomial of degree n, and let K be a splitting field for f. Prove that $[K : F]$ divides $n!$.

4 Modules

20. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\cup_{i=1}^{\infty} N_i$ is a submodule of M.

21. Let $R = \mathbb{Z}[x]$ and M be the ideal generated by 2 and x, viewed as an R-module. Show M is not free.

22. Let $V = \mathbb{Q}[x]/(x+1)^2 \oplus \mathbb{Q}[x]/(x-1)(x^2+1)^2 \oplus \mathbb{Q}[x]/(x+1)(x^2-1)$. Determine the invariant factors and elementary divisors for V.

23. Given an R-module M, we write $\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$.

Prove that if R is an integral domain, then $\mathrm{Tor}\, M$ is a submodule of M, and $\mathrm{Tor}(M/\mathrm{Tor}(M)) = 0$ (i.e. $M/\mathrm{Tor}(M)$ is torsion-free).

Give an example of a ring R and module M such that $\mathrm{Tor}\, M$ is not a submodule.

24. Prove $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \simeq \mathbb{Z}_{(n,m)}$.

25. Show that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

26. OOPs, I put a typo in!

    Show that $\mathrm{Hom}_R(\oplus A_i, B) \simeq \prod_i \mathrm{Hom}_R(A_i, B)$
    $\mathrm{Hom}_R(A, \prod B_j) \simeq \prod_j \mathrm{Hom}_R(A, B_j)$.

5 extra problems

1. Prove or give a counter example: If G is a finite group of order n and m is a positive integer dividing n, then G has a subgroup of order m.

2. Describe the kernel of the homomorphism from $\mathbb{R}[x] \to \mathbb{C}$ that takes a polynomial $f(x)$ to the complex number $f(i) = f(\sqrt{-1})$.

3. Let G be a group and p a prime number. Prove or give a counter example:

   (a) a group of order p is abelian.

   (b) a group of order p^2 is abelian.

   (c) a group of order p^3 is abelian.

4. Prove or give a counter example: If $1 \to K \to G \to H \to 1$ is an exact sequence of groups with both K and H abelian, then G is abelian.

5. Prove or disprove: $\mathbb{Z}[x]$ is a PID.

6 category theory

1. (a) In the category **Ab** of abelian groups, what is the coproduct $\mathbb{Z}/2\mathbb{Z} \sqcup \mathbb{Z}/2\mathbb{Z}$? What is their product $\mathbb{Z}/2\mathbb{Z} \sqcap \mathbb{Z}/2\mathbb{Z}$?

   (b) In the category **Gp** of groups, what is the coproduct $\mathbb{Z}/2\mathbb{Z} \sqcup \mathbb{Z}/2\mathbb{Z}$? What is their product $\mathbb{Z}/2\mathbb{Z} \sqcap \mathbb{Z}/2\mathbb{Z}$? What is the coproduct $\mathbb{Z} \sqcup \mathbb{Z}$?

   (c) In the category **Set** of sets, what is the coproduct of two sets? the product?

2. Let M be any left R-module. Show the covariant functor $\mathrm{Hom}_R(M, \cdot)$ is left exact.

   Show the contravariant functor $\mathrm{Hom}_R(\cdot, M)$ is left exact.

3. If the functor $\mathrm{Hom}_R(P, \cdot)$ is exact, we say P is a projective left R-module.

   If the functor $\mathrm{Hom}_R(\cdot, E)$ is exact, we say E is an injective left R-module.

   (a) Let $R = \mathbb{Z}$. Show the module $M = \mathbb{Z}$ is projective but that $N = \mathbb{Z}/7\mathbb{Z}$ is not.

   (b) Let $R = \mathbb{Z}$. Show the module $\mathbb{Q}$ is injective. Show the module $\mathbb{Q}/\mathbb{Z}$ is injective.

   (c) Let $R = \mathbb{Q}$. Show that all modules are projective and injective. (In fact, this is true over any field.)

4. Two functors $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$, $\mathfrak{G} : \mathfrak{D} \to \mathfrak{C}$ are *adjoint* to each other if for all objects $A \in \mathrm{Obj}(\mathfrak{C})$, $B \in \mathrm{Obj}(\mathfrak{D})$,

$$\mathrm{Hom}_{\mathfrak{C}}(A, \mathfrak{G}(B)) = \mathrm{Hom}_{\mathfrak{D}}(\mathfrak{F}(A), B).$$

   (a) Show these two functors are adjoint: $\mathfrak{F} : \mathbf{Gp} \to \mathbf{Ab}$, $G \mapsto G/G'$ (where G' is the commutator subgroup, i.e. $G/G' = G^{ab}$); $\mathfrak{G} : \mathbf{Ab} \to \mathbf{Gp}$, $A \mapsto A$.

   (b) Let R, S be rings, M a $R - S$-bimodule. Set $\mathfrak{F}(A) = M \otimes_S A$, $\mathfrak{G}(B) = \mathrm{Hom}_R(M, B)$. Show these are adjoint functors between R-modules and S-modules.

   (c) If you know about representation theory, let G be a group with subgroup H. Show induction Ind_H^G and restriction Res_H^G are adjoint functors between G-representations and H-representations. (this is also known as Frobenius reciprocity). In fact, even if you don't know representation theory, you can show this for the category of $\mathbb{C}G$-modules and $\mathbb{C}H$-modules, where $\mathrm{Ind}_H^G V = \mathbb{C}G \otimes_{\mathbb{C}H} V$.