PRACTICE PROBLEMS FOR ALGEBRA 259

Each of these problems (except those marked **Hard**) should take about 5-6 minutes for a rough solution, and not more than fifteen minutes for a complete written solution. The problems marked **Hard** should take about 10-15 minutes to solve and about 30 minutes for a full written solution.

For problems with multiple parts, the above time limits apply to each part. Also, for problems with multiple parts, an earlier part often needs to be used for the proof of a later part.

Problems marked **Very hard** are for fun only – no time limit.

These problems are meant to be tried *after* you are fairly thorough with the material. Do *not* waste time on problems marked **Hard** or **Very hard** if you are running short on time.

If you're finding these problems too hard for your taste, you might want to review some of the real homework, moral homework, in-class notes, and problem session material first.

1. Modules over principal ideal domains

1.1. The fundamental theorem.

(1) **Prove that** an integral domain is a principal ideal domain if and only if every finitely generated torsion-free module over it is free.

(2) Suppose R is a principal ideal domain that is not a field. **Prove that** the field of fractions of R is a torsion-free R-module that is not free. (For instance, the rational numbers are a torsion-free abelian group that is not free).

(3) Suppose R is a subring of the complex numbers containing 1, such that R is finitely generated as an abelian group. **Prove that**:
   (a) R is a free abelian group of finite rank, say n.
   (b) **Hard**: Every element of R satisfies a monic polynomial with integer coefficients of degree at most n.
   (c) The field of fractions of R is a finite extension of $\mathbb{Q}$ of degree n.

1.2. Jordan canonical form and rational canonical form.

Remember that the rational canonical form over a subfield remains a rational canonical form over bigger fields!

(1) Let K be a field. **Prove that** K is algebraically closed (i.e., every nonconstant polynomial has a root in K) if and only if every matrix over K is similar to an upper triangular matrix.

(2) A subgroup H of a group G is termed *conjugacy-closed* if any two elements of H that are conjugate in G are conjugate in H. **Prove that** if K is a subfield of a field L, then $GL_n(K)$ is conjugacy-closed in $GL_n(L)$ for any natural number n.

(3) Suppose K is a field, and suppose $A, B \in M_m(K), C \in M_n(K)$. Suppose the matrices:

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}, \qquad \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

are similar in $M_{m+n}(K)$. **Prove that** A and B are similar in $M_m(K)$.

(4) Suppose K is a field and suppose $A, B \in M_m(K)$. Suppose the matrices:

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \qquad \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}$$

are similar in $M_{2m}(K)$. **Prove that** A and B are similar in $M_m(K)$.

(5) Suppose K is an algebraically closed field:
   (a) **Prove that** the characteristic polynomial of a linear transformation has distinct roots if and only if the linear transformation can be expressed as a diagonal matrix with distinct diagonal entries.

(b) **Prove that** the minimal polynomial of a linear transformation has distinct roots if and only if the linear transformation can be expressed as a diagonal matrix.
(c) **Hard**: Suppose the characteristic of K is not 2, and suppose n is a natural number. **Prove that** there is a polynomial f in the n^2 matrix entries with the property that $f \neq 0$ for a matrix if and only if the matrix is diagonalizable with distinct diagonal entries.

2. Fields

Some of these problems may have solutions that use examples you have seen later in the course.

2.1. Funny fields.

(1) **Prove that** $\mathbb{R}$ contains a subfield isomorphic to $\mathbb{Q}(t_1, t_2, \dots)$, i.e., $\mathbb{R}$ contains a subfield isomorphic to the field of rational functions in countably many variables.
(2) **Prove that** the following fields have trivial automorphism groups:
   (a) The field of *real* algebraic numbers.
   (b) The field of real numbers constructible using straightedge and compass.
   (c) (Generalizing both the above): Any subfield of the field of reals that is closed under taking squareroots.
(3) **Give an example** of two isomorphic subfields of $\mathbb{R}$ that are finite extensions of $\mathbb{Q}$ but are not equal.

2.2. Imperial power and conservative roots.

(1) Suppose F is a field and p is a prime number. let F^* be the multiplicative group of F and $(F^*)^p$ be the subgroup comprising the p^{th} powers. **Prove that** the quotient group $(F^*)/(F^*)^p$ is isomorphic to the additive group of some vector space over the field of p elements.
(2) Suppose F is a field of characteristic not equal to two.
   (a) **Prove that** any quadratic extension of F can be written as $F(\alpha)$ where $\alpha^2 \in F$.
   (b) **Prove that** if $a, b \in F$ are such that ab is not a square, then $F(\sqrt{a})/F \ncong F(\sqrt{b})/F$ (i..e, they are not congruent as extensions).
   (c) Let F^* be the multiplicative group of F and $(F^*)^2$ be the subgroup of squares. **Prove that** the set of quadratic extensions of F (up to isomorphism) is in bijection with the set of non-identity elements of the group $(F^*)/(F^*)^2$.
(3) **Give an example** of a cubic extension of $\mathbb{Q}$ that does not contain any element outside $\mathbb{Q}$ whose cube is in $\mathbb{Q}$.
(4) Suppose F is a field of characteristic two.
   (a) **Prove that** a quadratic extension of F is inseparable if and only if it is of the form $F(\alpha)$ with $\alpha^2 \in F$.
   (b) **Prove that** a quadratic extension of F is separable if and only if it is the splitting field of an irreducible polynomial of the form $x^2 + x + a$ where $a \in F$.
(5) **Determine** all natural numbers n for which there exist irreducible polynomials of the form $x^n - a$ over a finite field with $q = p^k$ elements. (Reality check: the answer depends on q).
(6) (a) **Hard**: **Prove that** if G is a group with the property that for every natural number n, there are at most n elements whose order divides n, then every finite subgroup of G is cyclic.
   (b) **Prove that** any finite subgroup of the multiplicative group of a field is cyclic.

2.3. Block by block, brick by brick.

Burn your hands with these character-building problems!

(1) Suppose α and β have minimal polynomials $x^2 + ax + b$ and $x^2 + cx + d$ in $\mathbb{Q}[x]$. **Determine** the degrees and coefficients of the minimal polynomials of $\alpha + \beta$ and $\alpha\beta$ (note: the degree depends on the way the coefficients a, b, c, d are related).
(2) Dummit and Foote, Page 556, Section 13.6, Problem 13.

3. Galois theory

3.1. Change of variables.

(1) **Translation**: Let F be a field. For $a \in F$, define the map $t_a : F[x] \to F[x]$ given by $t_a(f(x)) = f(x-a)$. **Prove that** the map $a \mapsto t_a$ is a homomorphism from the additive group of F to the group of ring automorphisms of $F[x]$ fixing F pointwise. **Prove that** this map sends monic polynomials to monic polynomials and preserves degree. Further:
   (a) **Prove that** the splitting field of f is the same as the splitting field of $t_a(f)$ for any $a \in F$ and any monic polynomial $f \in F[x]$.
   (b) **Prove that** the discriminant of f equals the discriminant of $t_a(f)$ for any monic polynomial $f \in F[x]$.
   (c) Let n be the degree of f. If n is not a multiple of the characteristic of F, **prove that** there exists $a \in F$ such that the coefficient of x^{n-1} in $t_a(f)$ is zero.

(2) **Scaling**: Suppose F is a field and $a \in F^*$. Consider the following map from the set of monic polynomials in $F[x]$ to itself: $\mu_a(f(x)) = f(ax)/(a^{\deg(f)})$. **Prove that** this map sends monic polynomials to monic polynomials, is multiplicative, and preserves degree. Further:
   (a) **Prove that** the splitting field of f equals the splitting field of $\mu_a(f)$ for any monic nonconstant f and any $a \in F^*$.
   (b) **Prove that** the set of roots of $\mu_a(f)$ is obtained by multiplying each element of the set of roots of f by $1/a$.
   (c) **Determine** the ratio of the discriminants of f and $\mu_a(f)$. *Reality check*: The answer depends on the degree of f.
   (d) Let n be the degree of f. **Prove that**, if the coefficient of x^{n-1} in f is nonzero, there exists a such that the coefficient of x^{n-1} in $\mu_a(f)$ is 1.

(3) **Inversion**: Consider the following map i from the set of monic polynomials with nonzero constant term in $F[x]$ to itself: $i(f(x)) = x^{\deg(f)} f(1/x)/f(0)$. **Prove that** i sends monic polynomials with nonzero constant term to monic polynomials with nonzero constant term, is multiplicative, and preserves degree.
   (a) Let f be a monic polynomial with nonzero constant term. **Prove that** the splitting field of f equals the splitting field of $i(f)$.
   (b) **Determine** the relation between the set of roots of f and the set of roots of $i(f)$.
   (c) **Determine** the relation between the discriminant of f and the discriminant of $i(f)$.
   (d) **Prove that** if f has even degree, $f(0) = 1$, and $f = i(f)$, then we can write $f(x) = x^d g(x+1/x)$ for some polynomial g.

3.2. **The fundamental theorem.** Use group theory definitions and facts provided to answer the problems from field theory.

(1) Let p be a prime. **Prove that** a Galois extension of degree p^n is a composite of Galois extensions of degree p. *Group theory fact*: A group of order p^n has normal subgroups of order p^k for $0 \leq k \leq n$.

(2) Suppose G is the Galois group of a Galois extension K/F and H is a subgroup with fixed field E. **Determine**, in terms of K, E, and F, the fixed fields for the normal closure of H in G and the normal core of H in G. *Group theory definition*: The *normal closure* of a subgroup of a group is the smallest normal subgroup containing it, while the *normal core* of a subgroup is the largest normal subgroup contained in it.

(3) Suppose G is the Galois group of a Galois extension K/F and H is a subnormal subgroup of G with fixed field E. **Explore**: What information does this give about the extension E/F? *Group theory definition*: A subgroup H of a group G is subnormal if there exist subgroups $H = H_0 \leq H_1 \leq \cdots \leq H_n = G$ with each H_{i-1} normal in H_i.

(4) Suppose G is the Galois group of a Galois extension K/F and H is a subgroup of G with fixed field E. **Determine**, in terms of E and F, the fixed field of the normalizer $N_G(H)$. Also, **prove that** $N_G(H)/H$ is isomorphic to $\mathrm{Aut}(E/F)$.

(5) Suppose L is a Galois extension of a field F. Suppose K_1 and K_2 are intermediate Galois extensions of F. **Prove that** K_1K_2 and $K_1 \cap K_2$ are also Galois extensions of F. *Group theory fact*: A join of normal subgroups is normal, and an intersection of normal subgroups is normal.

(6) (a) **Prove that** if a real number α is contained in a Galois extension of $\mathbb{Q}$ whose degree is a power of 2, then α is constructible.

(b) **Find** a real number α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2 but α is not constructible. *Hint*: Use an irreducible polynomial of degree four whose Galois group is the symmetric group of degree four.

3.3. **More on polynomials, composition, and irreducibility.**

(1) Suppose F is a field and $f \in F[x]$ is a nonconstant monic polynomial such that for any $a \in F$, the polynomial $f(x) - a$ splits completely over F. Suppose $g \in F[x]$ is a nonconstant monic polynomial that splits completely over F. **Prove that** $g \circ f$ also splits completely over F.
(2) Suppose F is a field and $f(x) \in F[x]$ is a monic polynomial such that f splits completely over any field extension of F containing *any* root of f.
   (a) **Prove that** all irreducible factors of f have equal degree.
   (b) **Give an example** to show that f need not be irreducible.

4. Miscellaneous

4.1. **In search of truth.** Determine whether these innocuous-looking statements are true or false, and uncover the reasons.

(1) If K is a finite extension of a field F of degree $n > 1$, then K cannot be isomorphic to F as a field.
(2) Any finite extension of $\mathbb{Q}$ that is contained in $\mathbb{C}$ but not contained in $\mathbb{R}$ must contain a purely imaginary number.
(3) For every natural number n, there exists an irreducible polynomial over $\mathbb{Q}$ of degree n such that the Galois group of that polynomial has order n.
(4) Every finite group is isomorphic to a subgroup of the Galois group of some finite extension of $\mathbb{Q}$.
(5) If K is a finite Galois extension of F, there exists $\alpha \in K$ such that the set of conjugates of α in K over F forms a basis of K as a F-vector space.
(6) The polynomial $x^7 - 9$ is irreducible in $\mathbb{Q}[x]$.
(7) The polynomial $2x^7 + 2x^6 - 1$ is irreducible in $\mathbb{Q}[x]$.
(8) If α is a constructible real number, then every real number that is a Galois conjugate of α over $\mathbb{Q}$ is also constructible.