Mathematics 552 Algebra II Spring 2021

Final Problem Set

This is version 2′ (4/30/21 10:000 AM) of the final problem set. You should refer back to the class webpage periodically to see if any changes have been made, in which case a new version will be noted on the website.

You may use any books or references that you desire. Do not discuss the problems with anyone except me. You may email me with any questions that arise.

You should refer to the class website for any updates, corrections or the like for the exam.

The exam is due by 11:59 PM Friday, May 7. It can only be turned in in Canvas as the final problem set . Submit a pdf file with your solutions.

Explain your work clearly and carefully. You may just quote any results that were proved in class or in the sections of Jacobson. Be sure to carefully state the result that you are using.

1. Let $\mathbf{Q}^{alg}$ be the field of all complex numbers β such that the degree of the field extension $\mathbf{Q}(\beta)/\mathbf{Q}$ is finite. Let $\gamma \in \mathbf{Q}^{alg}$ be an element which is not in the rational field $\mathbf{Q}$.
   a) Show using Zorn's lemma that there is a subfield L of $\mathbf{Q}^{alg}$ which is maximal among subfields of $\mathbf{Q}^{alg}$ which do not contain γ.
   b) Let L be a maximal field as in a). Show that every finite degree extension E/L is a Galois extension with cyclic Galois group.

2. Let L/K be a Galois extension of fields of finite degree with $Gal(L/K) = G$ and the characteristic of K not 2.
   a) Let α and β be nonzero elements of L. Show that splitting fields for $x^2 - \alpha, x^2 - \beta$ over L are isomorphic (via an isomorphism which is identity on L) if and only if α/β is a square in L.
   b) Let γ be a nonzero element of L and let E/L be a splitting field of $x^2 - \gamma$ over L. Show that E/K is a Galois extension if and only if E/L is a splitting field for each of the polynomials $x^2 - g(\gamma)$ for all $g \in G$.
   c) Let $[L : K] = 2$ and let σ generate the Galois group of L/K. Show that if there is a degree 4 cyclic Galois extension E/K containing L/K as an intermediate extension then there exists an element of $t \in L$ such that $t\sigma(t) = -1$. Show that a quadratic imaginary extension of the field of rational numbers is not a subextension of a cyclic quartic field. Show that $\mathbf{Q}(\sqrt{2})$ is a subfield of a Galois field extension of the rationals with order 4 cyclic Galois group

d) Let $K = \mathbf{Q}, L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Let $\alpha^2 = (2+\sqrt{2})(2+\sqrt{3})(3+\sqrt{6})$ Show that $E = L(\alpha)$ is a Galois extension of the rational field $\mathbf{Q}$. Determine $Gal(E/\mathbf{Q})$.

3. Let n be a positive integer, let D be a division algebra and let $R = M_n(D)$ be the ring of $n \times n$ matrices with coefficients in D.

   a) Let $V = D^n$ be the irreducible left R-module of column vectors of length n with entries from D. Consider V as a left module over the opposite division ring D^{opp} via right multiplying the column vector by elements $d \in D$. For a D^{opp}-subspace $W \subset V$ let $I(W) = \{r \in R | rW = 0\}$. Show that $I(W)$ is a left ideal of R and that if t is invertible in R, then $I(tW) = I(W)t^{-1}$.

   b) Show that if $J \subset R$ is a left ideal, the set $V(J) = \{v \in D^n | Jv = 0\}$ is a D^{opp}-subspace of D^n and that for any invertible t in R we have $V(Jt^{-1}) = tV(J)$.

   c) Show that the maps in parts a) and b) give a bijection between left ideals of R and D^{opp} subspaces of D^n and that $\dim_D(I(W))/n + \dim_{D^{opp}}(W) = n$

   d) Give an example of a simple ring with exactly 12 non-zero proper left ideals

   e) Let S be a ring with exactly 11 non-zero proper left ideals. Show that S has at least one non-zero proper two-sided ideal.

4. Let F be a finite field with q elements, and let $f(x) \in F[x]$ be a polynomial.

   a) Show that the algebra $A = F[x]/(f(x))$ is a semisimple algebra if and only if $gcd(f(x), f'(x)) = 1$. When A is semisimple, describe A as a product of simple algebras in terms of the factorization of $f(x)$.

   For part b) and c) assume that $gcd(f(x), f'(x)) = 1$.

   b) Let T_k be the linear operator given by multiplication by $x^{q^k} - x$ on A. Show that the kernel of T_k has dimension over F equal to the sum of the degrees of all irreducible factors of $f(x)$ of degree dividing k. Explain how to compute the degrees of the irreducible factors of $f(x)$ by linear algebra on a finite dimensional vector space.

   c) Let U be the linear operator given by raising to q-th powers of elements in A. Show that the dimension of V_1, the eigenvalue 1 eigenspace of U, equals the number of distinct irreducible factors of $f(x)$. Show that if $h \in A$ is a nonzero eigenvector in this eigenspace V_1, then $\prod_{\alpha \in F}(h - \alpha) = 0$. If $f(x)$ is reducible, show that there exists a nonconstant polynomial $h(x) \in V_1$ and element $w \in F$ such that the greatest common divisor of $f(x)$ and $h(x) - w$ is a nonconstant proper factor of $f(x)$. Thus by linear algebra over the field F all information about the factorization of $f(x)$ is obtained.

5. Let G be a group for which there exists a field K such that the characteristic of K does not divide the order of G and the group ring $K[G]$ is a product of division rings. Show a),b),c) below to conclude that all subgroups of G are normal subgroups.

a) Let H be a subgroups of G and let $e = (1/|H|)\sum_{h\in H} h$. Show that $e^2 = e$ in $K[G]$.

b) Show that all idempotents of a ring which is a product of division rings are central.

c) Show using a), b) that all subgroups of G are normal subgroups. Give a non-abelian group such that the group ring is a product of division algebras.

6. Let S be a central simple algebra over a field K, and R a simple K-subalgebra of S. Let $C(R)$ denote the centralizer of R in S. Let $S \simeq M_n(D^{opp}) = End_D(L)$ where L is a simple $S-module$ and $D^{opp} = End_S(L)$. (Jacobson proves f) using Skolem-Noether. Do not use Jacobson's result in this problem.)

   a) Show that L is an $R\otimes D$ module. Show that the centralizer of R in $S = End_D(L)$ is $End_{R\otimes D}(L)$.

   b) Since $R \otimes D$ is simple, $R \otimes D \simeq End_E(W)$ where W is the unique simple $R \otimes D$ module and $E = End_{R\otimes D}(W)$ is a division algebra. Show that $L \simeq W^m$ as $R\otimes D$ modules for some m. Show that $C(R) \simeq End_{R\otimes D}(W^m) = M_m(End_{E\otimes D}(W)) \simeq M_m(E)$.

   c) Conclude that $C(R)$ is simple.

   d) Show that $S \simeq M_n(D^{opp})$ and $R \otimes D \simeq M_t(E^{opp})$ and $C(R) = M_m(E)$

   e) Show that dimension $[C(R) : K] = m^2[E : K]$ and $[L : K] = m[W : K] = m[W : E][E : K]$. Deduce that $[C(R) : K] = [L : K]^2/([R : K][D : K])$ and that $[R : K][C(R) : K] = [S : K]$.

   f) Deduce the double centralizer theorem $C(C(R)) = R$ by noting that the algebra $R \subset C(C(R))$ and from (e) applied to the subalgebra $C(R)$ that $[S : K] = [C(R) : K][C(C(R)) : K]$ so that $[C(C(R)) : K] = [R : K]$.

   The double centralizer theorem holds in many situations in other algebras.

7. Show as a corollary of the double centralizer theorem (part (f) above) that if R is a central simple algebra over a field K which is a subalgebra of a central simple algebra S over K then there is a K-algebra homomorphism $R \otimes_K C(R)$ onto S which is an isomorphism.