MAT 535 Review Sheet for Midterm 2

Remark. Some of these practice problems are harder than questions that would be asked on the midterm. If you are comfortable with these questions, then you will be well prepared for the final exam. This review sheet will be periodically updated as the semester continues.

Exam Policies. You must show up on time for all exams. Please bring your student ID card: ID cards may be checked, and students may be asked to sign a picture sheet when turning in exams. Other policies for exams will be announced / repeated at the beginning of the exam.

If you have a university-approved reason for taking an exam at a time different than the scheduled exam (because of a religious observance, a student-athlete event, etc.), please contact your instructor as soon as possible. Similarly, if you have a documented medical emergency which prevents you from showing up for an exam, again contact your instructor as soon as possible.

All exams are closed notes and closed book. Once the exam has begun, having notes or books on the desk or in view will be considered cheating and will be referred to the Academic Judiciary.

It is not permitted to use cell phones, calculators, laptops or other such electronic devices at any time during exams. If you use a hearing aid or other such device, you should make your instructor aware of this before the exam begins. You must turn off your cell phone, etc., prior to the beginning of the exam. If you need to leave the exam room for any reason before the end of the exam, it is still not permitted to use such devices. Once the exam has begun, use of such devices or having such devices in view will be considered cheating and will be referred to the Academic Judiciary. Similarly, once the exam has begun any communication with a person other than the instructor or proctor will be considered cheating and will be referred to the Academic Judiciary.

Review Topics.

Definitions. Please know all of the following definitions.

Finite ring homomorphism. Integral element. Integral ring homomorphism. Integral closure. Finitely generated ring homomorphism. Flat ring homomorphism. Faithfully flat ring homomorphism. Field. Fraction field. Field extension. Characteristic of a field. Prime subfield. Finite field extension. Algebraic field extension. Finitely generated field extension. Transcendence basis. Purely transcendental field extension.

Separable field extension. Separable polynomial. Inseparable field extension. Purely inseparable field extension. Field extension that splits a given finite separable extension. Splitting field. Algebraic element. Conjugate elements of an algebraic element. Algebraic closure of a field in an extension field. Algebraically closed field. Algebraic closure of a field. Normal field extension. Galois group. Fixed subfield of a group of field automorphisms. Cyclotomic extension. Finite field. Frobenius automorphism. Artin-Schreier extension.

Results. Please know all of the following lemmas, propositions, theorems and corollaries.

Integral closure. For every morphism of commutative rings, $u : R \to S$, an element of s is integral over R if and only if it generates a finite R-subalgebra of S if and only if it is contained in a finite R-subalgebra of S if and only if it satisfies a monic polynomial with coefficients in R. The integral closure of R in S is an R-subalgebra of S.

Finiteness of integral extensions. For every morphism of commutative rings, $u : R \to S$, such that evey element of S is integral over R, the R-algebra S is finite if and only if it is finitely generated.

Integral domain whose fraction field is an integral extension. For every integral domain R, for every element of the fraction field satisfying a monic polynomial over R with invertible constant coefficient, also the inverse of the element is integral over R. In particular, the integral closure of R in the fraction field equals the fraction field if and only if R already equals the fraction field.

Characteristic and prime subfields. For evey field F, either the unique morphism of rings from $\mathbb{Z}$ to F is injective and factors through the fraction field $\mathbb{Q}$ of $\mathbb{Z}$, or the morphism factors through a quotient field $\mathbb{Z}/p\mathbb{Z}$ for a prime integer $p(> 1)$. In the first case, the characteristic of F is defined to be 0. In the second case, the characteristic of F is defined to be $p(> 1)$.

Separability of a primitive extension. For every field extension $v : F \to E$, for every element x of E that is algebraic over v, the F-subextension $F[x]$ is separable over F if and only if the minimal polynomial $m_x^F(t)$ of x in $F[t]$ is separable, i.e., if and only if the formal derivative of $m_x^F(t)$ is a nonzero element of $F[t]$.

Separable closure. For every finite field extension $v : F \to E$, the set of elements x of E such that $F[x]$ is separable over F form an F-subextension L of E such that L is separable over F and E is purely inseparable over L.

Finite subgroups of multiplicative groups. For every field F, every finite subgroup of the multiplicative group $F^\times = F \setminus \{0\}$ is a cyclic group.

Existence of splitting fields. For every finite separable field extension $u : F \to L$ of some degree n, there exists a field extension $v : F \to E$ and a splitting of u, i.e., a set $\Sigma = (\sigma_1, \dots, \sigma_n)$ of n

pairwise distinct F-extensions, $\sigma_i : L \to E$, such that the induced E-algebra morphism

$$(\mathrm{Id}_E \otimes \sigma_1, \ldots, \mathrm{Id}_E \otimes \sigma_n) : E \otimes_F L \to \prod_{\sigma_i \in \Sigma} E,$$

is an isomorphism. Moreover, there exists such that v is minimal with this property, i.e., for every field extension $\widetilde{v} : F \to \widetilde{E}$ and for every splitting $\widetilde{\Sigma} = (\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_n)$ of u, there exists a (typically non-unique) morphism of F-extensions $w : E \to \widetilde{E}$ such that $\sigma_1 \circ f$ equals $\widetilde{\sigma}_1$. Also v is finite and separable. For all F-subextensions $K \subseteq L \subseteq E$, also L/K is finite and separable, and E/K splits L/K, i.e., E contains a splitting extension of L/K as a K-subextension.

Normal extensions. For every finite field extension $v : F \to E$ that is normal, i.e., v is separable and v splits itself, the group $\mathrm{Aut}_F(E)$ is a finite group of cardinality equal to the degree $[E : F] := \dim_F(E)$, and the subfield of E fixed by $\mathrm{Aut}_F(E)$ equals F. Moreover, for every F-subextension L of E that is also normal, the action of $\mathrm{Aut}_F(E)$ preserves L as a set (not necessarily pointwise), and the restriction homomorphism $\mathrm{Aut}_F(E) \to \mathrm{Aut}_F(L)$ is surjective with kernel equal to $\mathrm{Aut}_L(E)$.

Fundamental Theorem of Galois Theory. For every field E, for every finite subgroup G of the group of field automorphisms of E, the subfield F of E fixed by G gives a finite field extension, $v : F \to E$, whose degree equals the cardinality of G. The correspondence between the set of subgroups of G and the set of F-subextensions of E sending each subgroup H to the subfield $\mathrm{Fix}_H(E)$ of E fixed by H and sending every F-subextension L of E to $\mathrm{Aut}_L(E)$ is an order-reversing, bijective correspondence. Moreover, $[E : L]$ equals the cardinality of $\mathrm{Aut}_L(E)$, the degree $[E : \mathrm{Fix}_H(E)]$ equals the cardinality of H, and the correspondence identifies normal F-subextensions L of E with normal subgroups N of G so that $\mathrm{Aut}_F(L)$ equals $\mathrm{Aut}_F(E)/\mathrm{Aut}_L(E)$ is naturally isomorphic to the quotient group G/N.

Finite fields. For every prime integer $p(>1)$, for every positive integer e, there exists a finite field $\mathbb{F}_q = \mathbb{F}_{p^e}$, and this field is unique up to (typically non-unique) isomorphism. For every $q = p^e$ and for every positive integer d, there is a field extension $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^d}$, this is a normal extension, the Galois group is the cyclic group of order d generated by the iterated Frobenius automorphism Frob_E^e, and for every positive integer divisor c of d the fixed field of $(\mathrm{Frob}_E^e)^c$ is the unique $\mathbb{F}_q$-subextension $\mathbb{F}_{q^c}$ of $\mathbb{F}_{q^d}$. Moreover, the multiplicative group $(\mathbb{F}_{q^d})^\times$ is a cyclic group of order $q^d - 1$, for every generator x of this group, $\mathbb{F}_{q^d}$ equals the subextension $\mathbb{F}_q[x]$, and the separable polynomial $t^{q^d} - t$ factors in $\mathbb{F}_{q^d}$ into a product of distinct linear factors $\prod_{y \in \mathbb{F}_{q^d}} (t - y)$.

Eisenstein's Criterion. For every monic polynomial $m(t) = t^n + c_1 t^{n-1} + \dots + c_{n-1} t + c_n$ with coefficients c_k in the local ring $\mathbb{Z}_{p\mathbb{Z}}$, if p divides each element c_k, but p^2 does not divide c_n, then $m(t)$ is irreducible as an element in $\mathbb{Q}[t]$.

Cyclotomic extensions. For every integer n, the cyclotomic polynomial $\Phi_n(t) = \prod_{\zeta \in \mu_n^\times} (t - \zeta)$ is a monic polynomial in $\mathbb{Z}[t]$ of degree $\phi(n)$ that is irreducible in $\mathbb{Q}[t]$. (Here μ_n is the set of n^{th} roots

of unity in any splitting field of $t^n - 1$, and $\mu_n^\times$ is the set of generators of this order-n cyclic group.) The field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ of any root of $\Phi_n(t)$ is a splitting field of $\Phi_n(t)$ with Galois group naturally isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of multiplicatively invertible elements of the finite ring $\mathbb{Z}/n\mathbb{Z}$. The ring of integers in $\mathbb{Q}(\zeta_n)$ is **not** always a unique factorization domain.

Primitive Element Theorem. For every finite separable field extension, $u : F \to L$, there exists an element x in L such that L equals the F-subextension $F[x]$. There exist finite inseparable field extensions where this fails.

Practice Problems.

(1) For every degree-2 monic polynomial $m(t)$ over a field F, prove that $m(t)$ is irreducible unless $m(t)$ has a root in F. When $m(t)$ is irreducible, prove that $m(t)$ is separable unless the characteristic equals 2 and the linear term is zero. Whenever $m(t)$ is separable, prove that $F[t]/\langle m(t)\rangle$ is already a splitting field of $m(t)$, and describe the action of the Galois group with respect to the ordered F-basis $(1, \bar{t})$ in $F[t]/\langle m(t)\rangle$.

(2) For every degree-3 monic polynomial $m(t)$ over a field F, prove that $m(t)$ is irreducible unless $m(t)$ has a root in F. When $m(t)$ is irreducible, prove that $m(t)$ is separable unless the characteristic equals 3 and both the linear and quadratic terms are zero. Whenever $m(t)$ is separable, prove that $F[t]/\langle m(t)\rangle$ is a splitting field if and only if the discriminant is a square in F, in which case that Galois group is cyclic of order 3, i.e., it is isomorphic to the alternating group $\mathfrak{A}_3$. If the discriminant is not a square, prove that the splitting field is obtained from $F[t]/\langle m(t)\rangle$ by adjoining a square root of the discriminant. In this case, the Galois group acts as the entire symmetric group $\mathfrak{S}_3$.

(3) For every prime integer $p(>1)$, for every positive integer e, for every prime integer $\ell(>1)$, prove that the number of degree-ℓ, monic, irreducible polynomials in $\mathbb{F}_{p^e}[t]$ equals $(p^{e\ell} - p^e)/\ell$.

(4) For every prime integer $p(>1)$, for every positive integer e, for every prime integer $\ell(>1)$, for every positive integer d, prove that the number of degree ℓ^d, monic, irreducible polynomials in $\mathbb{F}_{p^e}[t]$ equals $(p^{e\ell^d} - p^{e\ell^{d-1}})/\ell^d$.

(5) Let ω be a primitive cubic root of unity in $\mathbb{C}$. Compute a minimal polynomial over $\mathbb{Q}$ of $x = \omega - \omega^{-1}$. What is the set of conjugate algebraic elements of x over $\mathbb{Q}$? What is the Galois group?

(6) Let x be $(1+i)\sqrt{2}$ in $\mathbb{C}$. Compute a minimal polynomial over $\mathbb{Q}$ of x. What is the set of conjugate algebraic elements of x over $\mathbb{Q}$? What is the Galois group? What are all of the subfields of the splitting field? What is the Galois group of x over $\mathbb{Q}(i)$?

(7) Let ζ be a primitive fifth root of unity in $\mathbb{C}$. Compute a minimal polynomial over $\mathbb{Q}$ of $x = \zeta - \zeta^{-1}$. What is the set of conjugate algebraic elements of x over $\mathbb{Q}$? What is the Galois group?

(8) We used the Primitive Element Theorem to simplify the proof of the Fundamental Theorem of Galois Theory for infinite fields F. Instead, assume the Fundamental Theorem of Galois Theory, and prove that every finite separable field extension of an infinite field is isomorphic to $F[t]/\langle m(t)\rangle$ for a monic, irreducible polynomial in $F[t]$.

(9) Let F be the field $\mathbb{C}(z)$ of rational functions in one variable, i.e., the field of holomorphic functions on the complement of finitely many points (depending on the holomorphic function) in the Riemann sphere $\mathbb{CP}^1$ that have finite order poles at each of the complementary points. For each integer d, let $m(t)$ be the monic polynomial $t^d + (z^d + 1)$. Use Eisenstein's criterion to prove that $m(t)$ is irreducible in $F[t]$. Compute the splitting field and the Galois group.

(10) Repeat the previous problem with the monic polynomial $m(t) = t^3 + z^3t + z$.

(11) This exercise is much easier to solve after studying complex functions of one variable. Let $m(t)$ in $\mathbb{C}(z)[t]$ be a degree-d, monic, irreducible polynomial whose discriminant is an element of $\mathbb{C}(z)$ each of whose zeroes and poles on the Riemann sphere $\mathbb{CP}^1$ is simple. Prove that the Galois group of $m(t)$ over $\mathbb{C}(z)$ acts as the full symmetric group on the n distinct roots of $m(t)$.

(12) Let F be the field $\mathbb{C}((z))$ of Laurent series in one variable. Prove that for every positive integer d, there exists a degree-d finite extension $F[z^{1/d}]$ of F, that this extension is unique up to (non-unique) isomorphism of F-extensions, and that the Galois group is a cyclic group of order d (canonically isomorphic to the order d cyclic group μ_d of roots of $z^d - 1$ in $\mathbb{C}^\times$). Index these fields by positive integers partially ordered by divisibility. Prove that the filtering colimit of these extension is an algebraic closure of $\mathbb{C}((z))$, the field of *Puiseux series*.

(13) Repeat the exercise above when F equals $k((z))$ where k is any algebraically closed field of characteristic 0, e.g., $\overline{\mathbb{Q}}$. However, this does not work for algebraically closed fields of positive characteristic. In positive characteristic, the correct variant of Puiseux series is *Hahn series*.

(14) Prove that there is no monic irreducible polynomial $m(t)$ in $\mathbb{C}(z)[t]$ whose discriminant has no zeroes or poles except at ∞.

(15) Prove that, for each positive integer e, there is a degree-p^e, monic, irreducible polynomial $m(t)$ of degree in $\overline{F}_p(z)[t]$ whose discriminant, considered as a rational function in z, has no zeroes or poles except at ∞. In fact, it is a theorem of David Harbater and Michel Raynaud (independently), that every finite p-group G can be the Galois group of some such $m(t)$ (whose degree depends on G). Thus the affine line in positive characteristic is wildly non-simply connected.

(16) Prove that the monic cubic polynomial $m(t) = t^3 - t - 1$ in $\mathbb{Q}[t]$ has a unique real root, called the *plastic number* (or *plastic ratio*). Even without computing the discriminant, prove that the Galois group acting on the roots of $m(t)$ is the full symmetric group on 3 elements, $\mathfrak{S}_3$.

(17) Let F be the field $\mathbb{Q}(p, q)$, and let $m(t)$ be the monic cubic polynomial $t^3 + pt + q$. Prove that $m(t)$ is irreducible in $F[t]$, and determine the Galois group.

(18) Now let F be the fraction field of $\mathbb{Q}[p,q,\Delta]/\langle \Delta^2 + (4p^3 + 27q^2)\rangle$. What is the Galois group of $m(t)$ over this field?

(19) Look up the formula for the "full discriminant" of the "general" cubic polynomial $m(t) = rt^3 + st^2 + pt + q$ (where r is not set to 1 and s set to 0 via a Tschirnhausen transformation). Look at the formula on the pedestal of the "Umbilic Torus" sculpture (by Helaman Ferguson) next to the Math Tower. What is the sculpture depicting? (The old-fashioned name is the "tangent developable of a twisted cubic".)

(20) Look up "cyclic codes". Why do computer scientists, electrical engineers, signals processing engineers, etc., care about Galois theory of finite fields?

(21) Let $p(>2)$ be an odd prime integer, let $\mathbb{F}_p$ be the prime field $\mathbb{Z}/p\mathbb{Z}$ of cardinality p, and let $v : \mathbb{F}_p \hookrightarrow E$ be a degree-p field extension. Prove that the minimal polynomial $m_x(t)$ over $\mathbb{F}_p$ of each element x of $E \smallsetminus v(\mathbb{F}_p)$ is $t^p - t - N(x)$ for some unique element $N(x)$ of $\mathbb{F}_p^\times$. Prove that the Galois orbit of x equals the coset $x + v(\mathbb{F}_p)$ inside E.

(22) Continuing the previous problem, prove that $N(x)$ equals the determinant of the $\mathbb{F}_p$-linear operator on E of multiplication by x. Thus, N extends to a group homomorphism from $E^\times$ to $\mathbb{F}_p^\times$ such that $N(y) = y^p = y$ for every element y of $\mathbb{F}_p^\times$. In particular, deduce that N is surjective.

(23) More generally, for every finite field, $\mathbb{F}_q$, with $q = p^e$ elements, for every degree-d field extension, $v : \mathbb{F}_q \hookrightarrow E$, prove that the determinant of the $\mathbb{F}_q$-linear operator on E of multiplication by x defines a group homomorphism N from $E^\times$ to $\mathbb{F}_q^\times$ that maps x to $x^{(q^d-1)/(q-1)}$. Since the domain of N is a cyclic group of order $q^d - 1$ and the target is a cyclic group of order $q-1$, deduce that N is surjective. This is an important observation in local class field theory.

(24) Let $\mathbb{Q}_p$ be the fraction field of the complete discrete valuation ring $\mathbb{Z}_p$ of p-adic integers. Let $E/\mathbb{Q}_p$ be the finite field extension $\mathbb{Q}_p[p^{1/d}]$, for an integer d that divides $p-1$. Prove that E is a Galois extension with cyclic Galois group isomorphic to the subgroup μ_d of d^{th}-roots of unity in $\mathbb{F}_p^\times$. Moreover, for the norm map from $E^\times$ to $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$, prove that the image in the quotient $\mathbb{Z}/p\mathbb{Z}^\times$ of $\mathbb{Z}_p^\times$ is a proper subgroup of index d. In local class field theory, we identify the Abelian extensions of a local field in terms of the image of the norm map in the multiplicative group of the local field.

(25) For the Archimedean local field $\mathbb{R}$, prove that we can also identify the finite, Galois extensions of $\mathbb{R}$ with Abelian automorphism group in terms of the image of the norm map.

(26) For the irreducible polynomial $m(t) = t^4 - t^2 + 1$ in $\mathbb{Q}[t]$, compute the Galois group as a subgroup of the symmetric group on the four roots of $m(t)$. Determine $\mathbb{Q}$-vector space bases of all subfields of the splitting field, together with generators of the corresponding subgroups of the Galois group. Determine which, if any, subfields admit an embedding into $\mathbb{R}$.

(27) For each prime integer $p(>1)$ different from 2 and 3, and for each positive integer e, for the prime power $q = p^e$ determine whether or not $m(t) = t^4 - t^2 + 1$ is irreducible in $\mathbb{F}_q$. If it factors,

determine the irreducible factors. If it is irreducible, determine the splitting field and the Galois group.

(28) For the irreducible polynomial $m(t) = t^6 + t^3 + 1$ in $\mathbb{Q}[t]$, compute the Galois group as a subgroup of the symmetric group on the six roots of $m(t)$. Determine $\mathbb{Q}$-vector space bases of all subfields of the splitting field, together with generators of the corresponding subgroups of the Galois group. Determine which, if any, subfields admit an embedding into $\mathbb{R}$.

(29) For each prime integer $p(> 1)$ different from 3, and for each positive integer e, for the prime power $q = p^e$ determine whether or not $m(t) = t^6 + t^3 + 1$ is irreducible in $\mathbb{F}_q$. If it factors, determine the irreducible factors. If it is irreducible, determine the splitting field and the Galois group.

(30) For the irreducible polynomial $m(t) = t^6 + 3$ in $\mathbb{Q}[t]$, compute the Galois group as a subgroup of the symmetric group on the six roots of $m(t)$. Determine $\mathbb{Q}$-vector space bases of all subfields of the splitting field, together with generators of the corresponding subgroups of the Galois group. Determine which, if any, subfields admit an embedding into $\mathbb{R}$.

(31) For each prime integer $p(> 1)$ different from 2 and 3, and for each positive integer e, for the prime power $q = p^e$ determine whether or not $m(t) = t^6 + 3$ is irreducible in $\mathbb{F}_q$. If it factors, determine the irreducible factors. If it is irreducible, determine the splitting field and the Galois group.

(32) Let the dihedral group $D_6 = \langle \rho, \sigma | \rho^3, \sigma^2, \sigma\rho\sigma\rho \rangle$ act on the field $E = \mathbb{C}(t)$ by $\rho \cdot t = 1/(1-t)$ and $\sigma \cdot t = 1/t$. The fixed field F is a subfield of a rational function field in one variable t over $\mathbb{C}$, hence F equals $\mathbb{C}(j)$ for some element j in $\mathbb{C}(t)$ by Lüroth's Theorem. Determine j. Also determine all F-subextensions of E together with their Galois groups.

(33) Repeat the previous problem with E equal to the field $\overline{\mathbb{F}}_p(t)$ for each prime integer $p(> 1)$ different from 2 and 3.

(34) Let the group $\mathfrak{S}_3$ of permutations on 3 letters acts on $E = \mathrm{Frac}(\mathbb{C}[t_1, t_2, t_3]/\langle t_1 + t_2 + t_3 \rangle)$ in the obvious way. The fixed subfield F is a subfield of the rational function field in two variables over $\mathbb{C}$, hence F equals $\mathbb{C}(s_2, s_3)$ for some elements s_2 and s_3 in E, by the two-dimensional analogue of Lüroth's Theorem (nota bene: the analogue of Lüroth's Theorem in transcendence degree ≥ 3 is false, as first proved by Clemens and Griffiths). Determine s_2 and s_3. Also determine all F-subextensions of E together with their Galois groups.

(35) Repeat the previous problem with E equal to the field $\overline{\mathbb{F}}_p(t)$ for each prime integer $p(> 1)$ different from 2 and 3.

(36) For each of the field extensions, $u : F \to L$, in the previous ten problems, find an element x in L such that L equals $F[x]$ (thus proving the Primitive Basis Theorem). For each Galois extension, $v : F \to E$, find an explicit isomorphism of the right $F^{\mathsf{Aut}_F(E)}$-module E with the right regular

representation on $F^{\mathsf{Aut}_F(E)}$ (thus proving the Normal Basis Theorem). Also determine the trace, the trace pairing, and the norm map.

(37) This is a very difficult problem. For the field $F = \mathbb{C}(t)$, for every finite extension of fields, $u : F \to L$, prove that the norm map Norm_F^L from $L^\times$ to $F^\times$ is surjective. This is a corollary of a theorem of Chiungtze C. Tsen, a doctoral student of Emmy Noether, who proved in his thesis what is now called Tsen's Theorem: the field $\mathbb{C}(t)$ is *quasi-algebraically closed* in the sense of Emil Artin. Much of Tsen's work on complex function fields was (temporarily) lost during World War II, and was independently discovered by Serge Lang in his doctoral thesis (who also proved in his thesis that the maximal unramified extension of each p-adic field is quasi-algebraically closed).

(38) For a field F, which field extensions, $u : F \to L$, can be realized as an F-subalgebra of the associative, unital F-algebra $\mathsf{Mat}_{n\times n}(F)$ of $n \times n$ matrices with entries in F. For each such embedding of L in $\mathsf{Mat}_{n\times n}(F)$, what is the relation between the characteristic polynomial of each element x of L and the minimal polynomial of x over F?

(39) For the field $\mathbb{Q}$, for the associative, unital $\mathbb{Q}$-algebra $\mathbb{H}_\mathbb{Q} := \mathbb{Q} \oplus \mathbb{Q}\cdot i \oplus \mathbb{Q}\cdot j \oplus \mathbb{Q}\cdot k$ of Hamilton quaternions whose coefficients are in $\mathbb{Q}$, which field extensions, $u : \mathbb{Q} \to L$, can be realized as a $\mathbb{Q}$-subalgebra of $\mathbb{H}_\mathbb{Q}$? If we extend from $\mathbb{Q}$ to the Galois extension field $\mathbb{Q}[\sqrt{-1}] := \mathbb{Q}[t]/\langle t^2+1\rangle$, what $\mathbb{Q}[\sqrt{-1}]$-algebra is $\mathbb{Q}[\sqrt{-1}] \otimes_\mathbb{Q} \mathbb{H}_\mathbb{Q}$?

(40) For the associative, unital $\mathbb{Z}$-algebra $\mathbb{H}_\mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}\cdot i \oplus \mathbb{Z}\cdot j \oplus \mathbb{Z}\cdot k$ of Hamilton quaternions whose coefficients are in $\mathbb{Z}$, for each prime integer $p(>1)$ other than 2, when is $\mathbb{F}_p \otimes_\mathbb{Z} \mathbb{H}_\mathbb{Z}$ a division algebra? The answer to this question is a theorem of Wedderburn that also follows as a corollary of a theorem of Chevalley (later extended by Warning to what is now called the Chevalley-Warning Theorem). For which prime integers $p(>1)$ other than 2 is the polynomial t^2+1 irreducible in $\mathbb{F}_p[t]$? Is it necessary for t^2+1 to factor in order to find an $\mathbb{F}_p$-algebra isomorphism of $\mathbb{F}_p \otimes_\mathbb{Z} \mathbb{H}_\mathbb{Z}$ with $\mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$?

(41) For a field F of characteristic different from 2, for a monic polynomial $m(t) = t^4 - at^2 + b$ in $F[t]$ that has no roots, prove that $m(t)$ is reducible if and only if both b is a square, $b = \beta^2$, and one of $a+2\beta$ or $a-2\beta$ is a square α^2. In this case, deduce that $m(t)$ factors as $(t^2 - \alpha t \pm \beta)(t^2 + \alpha t \pm \beta)$. In this case, the discriminant is $a - (\pm\beta)$, and a splitting field of $m(t)$ is obtained by adjoining the square root of the discriminant.

(42) For a field F of characteristic different from 2, for a monic irreducible polynomial $m(t) = t^4 - at^2 + b$ in $F[t]$, for a splitting field E of $m(t)$ over F, prove that the roots are of the form $\{+x_+, -x_+, +x_-, -x_-\}$ for elements x_+ and x_- in $E \smallsetminus F$. Deduce that b is the square of x_+x_- in E. Altogether, deduce that E contains a square root of b. Thus, after replacing F by $F[t]/\langle t^2 - b\rangle$, we may assume that b is a square.

(43) For a field F of characteristic different from 2, for a monic irreducible polynomial $m(t) = t^4 - at^2 + \beta^2$ in $F[t]$, since $m(t)$ equals $(t^2+\beta)^2 - (a+2\beta)t^2$, deduce that $a+2\beta$ is a square in E

but a nonsquare in F. Similarly, since $m(t)$ equals $(t^2-\beta)^2-(a-2\beta)t^2$, deduce that also $a-2\beta$ is a square in E but a nonsquare in F. If $a^2-4\beta^2$ is a square in F, say $a^2-2\beta^2=\gamma^2$, deduce that the splitting field of $m(t)$ is obtained by adjoining the square root of either $a+2\beta$ or $a-2\beta$ (these two field extensions are isomorphic). Write out the formulas for the four roots of $m(t)$, and determine the action of the Galois group.

(44) Continuing the previous problem, if also $a^2-4\beta^2$ is not a square in F, deduce that the splitting field of $m(t)$ equals a degree-4, biquadratic extension $F[\sqrt{a+2\beta},\sqrt{a-2\beta}]$ of F. Write out the formulas for the four roots of $m(t)$, and determine the action of the Galois group.

(45) Now put all of the pieces together. For a field F of characteristic different from 2, for a monic irreducible polynomial $m(t)=t^4-at^2+b$ in $F[t]$ such that b is not a square in F, prove that a splitting field E is either a degree-4 field extension of F if a^2-4b is a square in F, or it is a degree-8 field extension of F if a^2-4b is not a square in F. In the two cases, the Galois group of E of $F[\sqrt{b}]$ is either a cyclic group of order 2 or a Klein Viergruppe, i.e., isomorphic to a product of two cyclic groups of order 2. Write out formulas for the roots, and determine the action of the Galois group on these four roots.

(46) Let $\ell(>2)$ be a prime integer. Let F be a field whose characteristic is different from 2 and ℓ. Let b be an element of F that is not an ℓ^{th} power. Prove that the splitting field E of the monic polynomial $m(t)=(t^2-a)^\ell-b$ contains the splitting field K of $t^\ell-b$. For one root β of $t^\ell-b$ in K, if $a+\beta$ is a square in K, prove that for every root β', also $a+\beta'$ is a square in K. Thus, either $m(t)$ splits completely in K, or $m(t)$ has no roots in K.

(47) Continuing the previous exercise, if $a+\beta$ is a square in K, deduce that it is even a square in $F[\beta]$. By computing the matrix representative relative to the basis $\{1,\beta,\dots,\beta^{\ell-1}\}$, deduce that the determinant of the matrix of $a+\beta$ is also a square in F, i.e., $a^\ell+(-1)^\ell b$ is a square in F. Since ℓ is an odd integer, this is $a^\ell-b$. For the monic irreducible polynomial $m(t)=(t^2-2)^3-2$ in $\mathbb{Q}[t]$, deduce that the splitting field is strictly larger than $\mathbb{Q}[\sqrt[3]{-11},\omega]$, where ω is a root of t^2+t+1.

(48) Find a splitting field of the monic, irreducible polynomial $((t^2-1)^3+1)/t^2$, i.e., t^4-3t^2+3 in $\mathbb{Q}[t]$.

(49) Find a splitting field of the monic, irreducible polynomial $((t^2-1)^5+1)/t^2$, i.e., $t^8-5t^6+10t^4-10t^2+5$ in $\mathbb{Q}[t]$.

(50) Find a splitting field of the monic, irreducible polynomial $((t^5-1)^3+1)/t^5$, i.e., $t^{10}-3t^5+3$ in $\mathbb{Q}[t]$.

(51) Find a finite extension of fields that does not have a primitive generator.

(52) For every field extension, $F\xrightarrow{u}L$, for every F-vector space V, for every subset $\mathcal{B}$ of V, prove that $\mathcal{B}$ is an F-vector space basis of V if and only if the image $\{1\}\otimes\mathcal{B}$ in $L\otimes_F V$ is an L-vector

space basis of $L \otimes_F V$. Deduce that the F-vector space dimension of V equals the L-vector space dimension of $L \otimes_F V$.

(53) For every field extension, $F \xrightarrow{u} L$, for every F-linear transformation of F-vector spaces, $T : V \to W$, prove that T is injective, respectively surjective, bijective, if and only if also $\mathsf{Id}_L \otimes_F T$ is an injective, resp. surjective, bijective, L-linear transformation from the L-vector space $L \otimes_F V$ to the L-vector space $L \otimes_F W$.

(54) For every field extension, $F \xrightarrow{u} L$, for every partially ordered set $(I, \leq)$, for every compatible system of F-vector spaces, $((V_i)_{i \in I}, (T^i_j)_{(i,j) \in I^2, i \leq j})$, for every directed limit (i.e., colimit) of this compatible family, $(T^i_\infty : V_i \to V_\infty)_{i \in I}$, prove that also $(\mathrm{Id}_L \otimes_F T^i : L \otimes_F V_i \to L \otimes_F V_\infty)$ is a directed limit of the compatible family of L-vector spaces, $((L \otimes_F V_i)_{i \in I}, (\mathrm{Id}_L \otimes_F T^i_j)_{(i,j) \in I^2, i \leq j})$.

(55) For every field extension, $F \xrightarrow{u} L$, for every F-linear transformation $T$from an F-vector space V to an F-vector space W, prove that T equals zero if and only if the base change $\mathrm{Id}_L \otimes_F T$ from $L \otimes_F V$ to $L \otimes_F W$ equals zero.