Problems 1–9. Finite and algebraic extensions. (Assume that E is a field extension of the field F.)

Definition 1. Suppose E is an extension field of the base field F. We say that E is a *finite extension* of F if the dimension $[E : F]$ is finite. The dimension $[E : F]$ is also called the *degree* of the field extension E over F. We say that E is an *algebraic extension* of F if *every* element of E is algebraic over F.

1. Recall that E is a vector space over F (why?). Show that if the dimension $n = [E : F]$ is finite then E is an algebraic extension of F. In fact, every $\alpha \in E$ is a root of a nonzero polynomial in $F[X]$ of degree at most n. Hint: can $1, \alpha, \alpha^2, \ldots, \alpha^n$ be linearly independent?

2. Show that $\mathbb{C}$ is an algebraic extension over $\mathbb{R}$, but not over $\mathbb{Q}$. Hint: for $\mathbb{Q}$ the dimension is infinite, but that is a red herring. Use famous theorems about π and/or e instead.

3. Suppose that L is a finite extension of E with basis $\ell_1, \ldots, \ell_m$, and suppose that E is a finite extension of F with basis $e_1, \ldots, e_n$. Show that elements of the form $e_i \ell_j$ form a basis for L as an F-vector space. Conclude that $[L : F] = [L : E][E : F]$.

4. Suppose that R is an integral domain containing the field F. Then R is a F-vector space. Show that if the dimension is finite, then R is a field. Hint: if $v_1, \ldots, v_n \in R$ is a basis and $\alpha \neq 0$ then the vectors $\alpha v_1, \ldots, \alpha v_n$ are linearly independent, so must be a basis; write 1 in terms of this basis.

5. Show that $\alpha \in E$ is algebraic over F if and only if $F[\alpha]$ is a field of finite dimensional over F.

6. Show that if $\alpha_1, \alpha_2, \ldots \alpha_n \in E$ are algebraic over F, then $F[\alpha_1, \alpha_2, \ldots \alpha_n]$ is a field of finite dimension over F.

7. Using the previous problem, show that if $\alpha, \beta \in E$ are algebraic over F, then so are their sum and product. Show that if $\alpha \in E$ is algebraic over F and nonzero, then α^{-1} is algebraic over F. Conclude that the subset of all elements of E that are algebraic over F forms a subfield of E.

8. Show that if L is an algebraic extension of E, and E is an algebraic extension of F, then L is an algebraic extension of F. Hint: if $\alpha \in L$ has minimal polynomial $g \in E[X]$, let $\beta_0, \beta_1, \ldots, \beta_{n-1}$ be the coefficients of g. What do you know about $[E_0[\alpha] : E_0]$ and $[E_0 : F]$ for $E_0 = F[\beta_0, \beta_1, \ldots, \beta_{n-1}]$?

9. Suppose E is a finite extension of F. Show that $[E : F] = 1$ if and only if $E = F$.

Problems 10–11. Algebraically closed fields. (Let F be a field)

Definition 2. Let E be an extension field of the field F. We say that E is an *algebraic closure of F* if (i) E is algebraic over F, and (ii) there is no field extension E' of E with $E' \neq E$ that is algebraic over F.

Definition 3. We say that a field E is *algebraically closed* if every irreducible polynomial $f \in E[X]$ is linear. Thus E is algebraically closed if and only if every nonconstant polynomial in $E[X]$ has a root.

10. Show that if E is an algebraic closure of F if and only if (i) E is algebraic over F, and (ii) E is algebraically closed.

11. Show that if F is a subfield of an algebraically closed field E, then E contains a unique subfield that is an algebraic closure of F. For example, the fundamental theorem of algebra says $\mathbb{C}$ is algebraically closed. Thus $\mathbb{Q}$ has a unique algebraic closure $\overline{\mathbb{Q}}$ in $\mathbb{C}$.

It turns out that algebraic closures exist for any F and are unique up to isomorphism. (We will not really need the uniqueness, but it is an important result to know).

Fact. *Every field F has an algebraic closure. Any two algebraic closures of F are isomorphic with an isomorphism fixing F.*

Problems 1–3. Splitting fields. (Let F be a field, which we call the base field.)

Definition 1. Let E be a field. If $f \in E[X]$ is a nonconstant polynomial that factors into linear factors in $E[X]$, then we say that f *splits* in E.

Definition 2. Let E be a field extension of F. Let $f \in F[X]$ be a nonconstant polynomial. Then E is a *splitting field of f over F* if (i) f splits in E, and (ii) $E = F[\alpha_1, \ldots, \alpha_n]$ where α_i are the roots of f in E.

1. Let $f \in F[X]$ be a nonconstant polynomial, and let L be a field extension of F in which f splits. Show that there is a unique subfield of L that is a splitting field of f over F. This applies, for example, if L is an algebraically closed field containing F.

2. Show that there is a splitting field for any nonconstant $f \in F[X]$. Hint: use the above where L is an algebraically closed field containing F. For example, if $F = \mathbb{Q}$ you can work in $\mathbb{C}$. Your can also construct a splitting field directly without assuming the existence of such an L: let $F_1 = F[X]/\langle f_1 \rangle$ where f_1 is a nonlinear irreducible factor of f. Then form a sequence $F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq \cdots$ in a similar way until you reach a splitting field. Later we will show that two splitting fields are isomorphic (with an isomorphism fixing F), so the actual method of construction is not so critical.

3. Show that splitting fields are finite-dimensional extensions of the base field.

Problem 4–5. Galois extensions. (Let F be a field, which we call the base field)

Definition 3. Let E be a finite extension of F. We say that E is a *Galois extension* of F if there is a nonconstant $f \in F[X]$ with no multiple roots in E such that E is the splitting field of f over F.

For such an extension E, the *Galois group* $\mathrm{Gal}(E/F)$ of E over F is the group of (ring) automorphisms of E that fix the base field F.

Let H be a subgroup of the Galois group G. The *fixed field of H*, written E^H, is defined to be the set of elements of E fixed by every $g \in H$.

4. Let E be a finite Galois extension of F. Verify that the Galois group is indeed a group under composition. (We will later see that this group is finite.) Let H be a subgroup of the Galois group. Show that E^H is indeed a field extension of F contained in E. (Later we will show that $E^G = F$.)

5. Show that $\mathbb{Q}[\sqrt{d}\,]$ is Galois over $\mathbb{Q}$. Show that $\mathbb{Q}[2^{1/4}, i]$ is Galois over $\mathbb{Q}$. Show that if $\zeta_6 \in \mathbb{C}$ is a primitive sixth root of unity, then $\mathbb{Q}[\zeta_6]$ is Galois over $\mathbb{Q}$. Show that if E is a finite field of characteristic p, then E is Galois over $\mathbb{F}_p$. (Hint: find a polynomial with E as its set of roots).

Problems 6–9. Extensions of homomorphisms. (Let $\phi : R_1 \to R_2$ be a homomorphism between commutative rings with unity.)

6. Explain why ϕ extends to a unique homomorphism $\phi_X : R_1[X] \to R_2[X]$ that sends X to X. If ϕ is injective, show that ϕ_X is a degree-preserving injection. If ϕ is an isomorphism, show that ϕ_X is an isomorphism. When $\phi\colon F_1 \to F_2$ is an isomorphism between fields, explain how the factorization of a nonzero polynomial $f \in F_1[X]$ in $F_1[X]$ is related to the factorization of $\phi_X f$ in $F_2[X]$.

7. Given $f \in R_1[X]$ and $\alpha \in R_1$, show that $\phi\big(f(\alpha)\big) = (\phi_X f)(\phi\,\alpha)$. Conclude that if α is a root of f, then $\phi(\alpha)$ is a root of $\phi_X f$.

8. For any $f \in R_1[X]$, construct a homomorphism $R_1[X]/\langle f \rangle \to R_2[X]/\langle \phi_X f \rangle$. Show that if ϕ is an isomorphism, then the resulting homomorphism on quotients is also an isomorphism. Hint: first form the composition $R_1[X] \to R_2[X] \to R_2[X]/\langle \phi_X f \rangle$.

9. Suppose $\phi : F_1 \to F_2$ is an isomorphism between fields, and that $f \in F_1[X]$ is irreducible. Let E_1 be an extension of F_1 containing a root α of f. Let E_2 be an extension of F_2 containing a root β of $\phi_X f$. Show there is a unique isomorphism $F_1[\alpha] \to F_2[\beta]$ that extends ϕ and sends α to β.

GT 3

June 2003 (Revised July 2019)

Our goal is to prove the following "extension lemma", and then derive significant consequences.

Lemma. *Let $f \in F[X]$ be a nonconstant polynomial where F is a field. Let E and E' be splitting fields of f over F. Let L be a subfield of E that contains F. Then every homomorphism $\phi : L \to E'$ fixing F can be extended to a homomorphism $E \to E'$. If f does not have multiple roots in E', then there are exactly $[E : L]$ such extensions. (In general, whether or not f has multiple roots, $[E : L]$ is an upper bound.)*

Problems 1–4. Proof of the lemma. (Assume F, f, E, E', L, and ϕ are as above.)

1. Suppose that $\alpha \in E$ is a root of f. Let f_1 be the minimal polynomial of α over L. We know from GT 2.7 that any extension of ϕ to $L[\alpha] \to E'$ must map α to a root of $\phi_X f_1$. Conclude that the number of such extensions is bounded by the number of roots of $\phi_X f_1$ in E'.

2. Let α and f_1 be as above. Show that $\phi_x f_1$ is a polynomial of degree $\big[L[\alpha] : L\big]$ that divides f in $E'[X]$. Show that it has at least one root in E' and at most $\big[L[\alpha] : L\big]$ roots in E'. Show that it has exactly $\big[L[\alpha] : L\big]$ roots if f does not have multiple roots in E'.

3. Let α and f_1 be as above. Let L' be the image of L under ϕ. For any root β of $\phi_X f_1$, use GT 2.9 to show that there is a unique extension $L[\alpha] \to L'[\beta]$ of the isomorphism $L \to L'$ that sends α to β. Conclude that the total number of homomorphisms $L[\alpha] \to E'$ extending ϕ is equal to the number of distinct roots of $\phi_x f_1$ in E'.

4. Prove the lemma. Hint: induction on $[E : L]$. If E is not L then consider E over $L[\alpha]$ where α is a root of f in E but not in L. Use 1–3 above to consider extensions from L to $L[\alpha]$, and the induction hypothesis to move from $L[\alpha]$ to E.

Problems 5–10. Consequences of the lemma. (Let F be a field.)

5. Suppose E and E' are splitting fields of a nonconstant polynomial $f \in F[X]$. Show that any homomorphism $\phi\colon E \to E'$ fixing F is actually an isomorphism. Furthermore, number of distinct roots of f is the same in E and E'. Hint: Let E'' be the image. Observe that $f = \phi_X f$ must factor into linear factors in $E''[X]$, and the number of distinct factors is the same in $E''[X]$ and $E[X]$.

6. Conclude that any two splitting fields E, E' of a polynomial $f \in F[x]$ are isomorphic with an isomorphism fixing the base field. Show that if f has distinct roots in E (or equivalently in E'), then there are exactly $[E : F]$ such isomorphisms. Conclude also that $[E : F] = [E' : F]$.

7. Prove the following.

Theorem. *If E is a finite Galois extension of F, then there are exactly $[E : F]$ elements in the Galois group of E over F.*

8. Suppose that E is a finite Galois extension of F and that L is an intermediate field between F and E. Show that E is Galois over L, and that $\mathrm{Gal}(E/L)$ is a subgroup of $\mathrm{Gal}(E/F)$.

9. Prove the following. (Hint: $[E : E^G][E^G : F] = [E : F]$. Show that $[E : E^G] = |G| = [E : F]$ by the earlier theorem. Why is $\mathrm{Gal}(E/E^G) = G$?)

Theorem. *Suppose E is a finite Galois extension of F, and that G is the Galois group of E over F. Then $E^G = F$.*

10. Show that if E is a splitting field over F, and L is an intermediate field between F and E, then any automorphism of L fixing F can be extended to an automorphism of E.

Definition 1. Let E be a finite Galois extension of F with Galois group G. Let $\alpha \in E$. Then any element of the form $\sigma\alpha$ with $\sigma \in G$ is called a *G-conjugate* of α (or simply a *conjugate* of α if G is clear from context).

Problems 1–3. Conjugates. (Let E be a finite Galois extension of F with Galois group G.)

1. Show that $\alpha \in E$ has at most $[E : F]$ conjugates, and is in F if and only if it has only 1 conjugate.

2. Suppose that $\alpha \in E$ has minimal polynomial $f \in F[X]$ over F. Show that any conjugate of α is a root of f. (We will show every root is a conjugate later). Conclude that if $\sigma \in G$, then $X - \sigma\alpha$ divides f in $E[X]$.

3. Let $\alpha \in E$, and let $H = \{\sigma \in G \mid \sigma\alpha = \alpha\}$. Show that H is a subgroup of G. Given $\sigma, \tau \in G$, show that $\sigma\alpha = \tau\alpha$ if and only if $\sigma H = \tau H$ as cosets. Show that the map $\sigma H \mapsto \sigma\alpha$ is a (well-defined) bijection between the (left) cosets of H and the G-conjugates of α. Conclude that the number of G-conjugates of α is $[G : H]$. Conclude that the number of G-conjugates of α divides $[E : F]$.

Problems 4–5. Minimal Polynomial Formula. (Let E be a finite Galois extension of F with Galois group G. Let $\alpha \in E$, and let $\alpha_1, \ldots, \alpha_m$ be the distinct G-conjugates of α).

4. Let f be the minimal polynomial of α in $F[X]$. Show that $\prod_{i=1}^m (X - \alpha_i)$ divides f in $E[X]$.

5. Let $\sigma \in G$. Show that σ permutes the set of conjugates $\{\alpha_1, \ldots, \alpha_m\}$. Let $h = \prod_{i=1}^m (X - \alpha_i)$. Show that $\sigma_X h = h$. Conclude that $h \in F[X]$. Now prove the following theorem and corollary:

Theorem. *Let E be a finite Galois extension of F with Galois group G. Let $\alpha_1, \ldots, \alpha_m$ be the G-conjugates of $\alpha \in E$. Then the minimal polynomial f of α in $F[X]$ is*

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i).$$

Corollary. *Let E be a finite Galois extension of F. If $f \in F[X]$ is irreducible, and if at least one root of f is in E, then f splits in E and f has distinct roots in E.*

Problems 6–10. Galois group as a permutation groups. (Let E be a finite Galois extension of F with Galois group G.)

6. Let f be a polynomials that splits in E. Show that each element of G permutes the roots of f. Thus if we number the roots of f as $1, 2, \ldots, m$ then each element of G can be assigned to a permutation in $\mathcal{S}_m$. Show that the map $G \to \mathcal{S}_m$ is a homomorphism.

7. Let f be chosen so that E is the splitting field of f over F. Show that the homomorphism $G \to \mathcal{S}_m$ discussed above is injective. So, in this case, we can represent G as a subgroup of $\mathcal{S}_m$.

8. Show that if f is an *irreducible* polynomial in $F[x]$ that splits in E, then G acts transitively on the roots of f. Thus the image of G in $\mathcal{S}_m$ acts transitively on $\{1, 2, \ldots, m\}$. (*G acts transitively on a set* means that given any two elements of the set, you can find an element of G that maps the first element to the second.)

9. Suppose that E is the splitting field of an irreducible cubic $f \in F[x]$ (with distinct roots). Use Problems 6–8 above to the represent the Galois group as a subgroup of $\mathcal{S}_3$. List the possible subgroups of $\mathcal{S}_3$. What about if f is an irreducible quadratic?

10. Let $E = \mathbb{Q}\left(2^{1/4}, i\right)$. Show that E is Galois over $\mathbb{Q}$, and that its Galois group G has 8 elements. (Hint: what is the degree of $\mathbb{Q}\left(2^{1/4}\right)$ over $\mathbb{Q}$?) Describe G explicitly based on the images of $2^{1/4}$ and i. Describe how the elements of G permute the roots of $X^4 - 2$. Now relate G to the symmetries of the square (the dihederal group with 8 elements), and conclude that G is isomorphic to this dihederal group.

Our next goal will be to prove the following.

Theorem (Primitive Element Theorem)**.** *Let L be an extension of F. If there is a finite Galois extension E of F containing L, then there is an element $\alpha \in L$ such that $L = F[\alpha]$.*

Problems 1–3. Intermediate fields. (Let E be a finite Galois extension of F with Galois group G.)

1. Let L be an intermediate field between F and E. Recall that E is Galois over L, and that the Galois group of E over L is the following subgroup:

$$G_L \stackrel{\text{def}}{=} \{\sigma \in G \,|\, \sigma\beta = \beta \text{ for all } \beta \in L\}.$$

Observe that the map $L \mapsto G_L$ maps the set of intermediate subfields between F and E to the finite set of subgroups of G.

2. Suppose L and L' are intermediate fields between F and E. Show that if $L \neq L'$ then $G_L \neq G_{L'}$. Hint: Suppose $G_L = G_{L'}$. So $E^{G_L} = E^{G_{L'}}$. Now use a previous theorem.

3. Show that there are only a finite number of intermediate fields between F and E.

Problem 4–6. Some linear algebra. (Let V be a vector space over F.)

4. Consider the set $\{u + t(v - u) \mid t \in F\}$ where $u, v \in V$. We call such a set a "line". Given a subspace $W \subseteq V$ and such a line, show that either the line is contained in W, or intersects W in at most one point.

5. Let W_1 and W_2 be two distinct proper subspaces of V. Show that there is a vector $w \in V$ which is not in the union of W_1 and W_2. (Hint: let $u \notin W_1$ and $v \notin W_2$. Consider the associated line. How does this line intersection W_1 and W_2? If $F = \mathbb{F}_2$ then a separate argument must be given.)

6. Generalize the above to the following proposition. How is the assumption that F is infinite used in your proof? Hint: use induction, and lines.

Proposition. *Let V be a vector space with infinite scalar field F. Let $W_1, \ldots, W_n$ be a finite collection of proper subvector spaces. Then there is a vector of V not in the union $\bigcup W_i$.*

Problem 7–9. The Primitive Element Theorem. (Let E be a finite Galois extension of F.)

7. Suppose F is infinite. Let L be an intermediate field between F and E. Show that $L = F[\alpha]$ for some $\alpha \in L$. Hint: use the above proposition with $V = L$.

8. Prove that the primitive element theorem holds for finite F as well. Hint: use the following fact.

Fact. *If F is a field then any finite subgroup of $F^\times$ is cyclic.*

9. Let $E = \mathbb{Q}\left[2^{1/4}, i\right]$ as in Problem 10 of GT4. Find $\alpha \in E$ such that $E = \mathbb{Q}[\alpha]$. Hint: find $\alpha \in E$ such that $\sigma\alpha \neq \alpha$ for all non-identity elements $\sigma \in G$. Show that such α cannot be in a proper subfield L of E intermediate between $F$and E.

GT 6

June 2003 (Revised July 2019)

Problems 1–5. Multiple roots and derivatives. Perfect fields. (Let F be a field.)

Proposition. *Suppose $f \in F[X]$ splits in an extension E and $f \neq 0$. Then f has a multiple root in E if and only if $\gcd(f, f')$ is of positive degree.*

Corollary. *Suppose $f \in F[X]$ is irreducible and splits in an extension E. Then f has multiple roots in E if and only if $f' = 0$.*

Definition 1. Suppose $f \in F[X]$ is nonzero. If f splits with distinct roots in an extension E we say f is *separable*. So if f is irreducible, f is separable if and only if $f' \neq 0$. The field F is called *perfect* if $f' \neq 0$ for all irreducible $f \in F[X]$.

1. Prove the above proposition and corollary.

2. Describe the polynomials $f \in F[X]$ with $f' = 0$. (In both characteristic 0 and positive characteristic). Conclude that any field of characteristic 0 is perfect.

3. Suppose that F is a field of characteristic $p > 0$, and that $F^p = F$ where F^p be the set of pth powers. Show, for all $f \in F[X]$, that $f' = 0$ if and only if f is of the form $(f_0)^p$ for some $f_0 \in F[X]$. Conclude that every irreducible polynomial has nonzero derivative, and that F is perfect.

4. On the other hand, suppose $F^p \neq F$ where F has characteristic $p > 0$. Let $c \in F$ where $c \notin F^p$. Show $X^p - c$ is irreducible and has zero derivative. Conclude that F is not perfect. Hint: If r, in some extension E, is a root, then $c = r^p$. So $r \notin F$, but $X^p - c = (X - r)^p$ in $E[x]$. Suppose that $g \in F[x]$ is an irreducible factor, so g factors as a power of $(X - r)$ in $E[x]$. So g has multiple roots. Now use the Corollary to show that g has degree p.

5. Let F be a field of characteristic $p > 0$. Show that $X^p - 1 = (X - 1)^p$, and conclude that the homomorphism $x \mapsto x^p$ is an injection $F^\times \to F^\times$. If F is finite, show it is a surjection. Show that if F is finite then $F^p = F$, and so F is perfect. Hint: what is the kernel of $x \mapsto x^p$?

Problems 6–9. Separable extensions. (Let F be a field and let E be a finite extension of F.)

Definition 2. An algebraic extension L of F is called *separable* over F if the minimal polynomial in $F[X]$ of every element of L is separable.

6. Suppose E is Galois over F. Show that any intermediate L with $F \subseteq L \subseteq E$ is separable over F.

7. Show that a nonconstant $f \in F[X]$ is separable if and only if it factors into distinct (nonassociate) separable irreducible polynomials. Suppose $L = F[\alpha_1, \ldots, \alpha_n]$ where the minimal polynomial of each α_i in $F[X]$ is separable. Show that L is contained in a finite Galois extension of F, and that L is separable.

8. Prove the following:

Proposition. *Let L be a finite extension of F. The following are equivalent.*

1. *L is separable over F.*
2. *L is contained in a finite Galois extension of F.*
3. *$L = F[\alpha]$ where the minimal polynomial of α in $F[X]$ is separable.*

9. Show that if F is perfect, then any algebraic extension of F is separable.

GT 7

June 2003 (Revised July 2019)

Problems 1–3. Subgroups are Galois groups. (Let E be a finite Galois extension of F with Galois group G. Let H be a subgroup of G, and let E^H be the fixed field of H.)

1. Show that H is a subgroup of $\mathrm{Gal}\big(E/E^H\big)$.

2. Let $\alpha \in E$ be such that $E = F[\alpha]$. Note that $E = E^H[\alpha]$. Consider the following polynomial

$$g \stackrel{\text{def}}{=} \prod_{\sigma \in H} \big(X - \sigma(\alpha)\big).$$

Show that $g \in E^H[X]$. Use results of GT4 to show that g divides the minimal polynomial of α over E^H, hence g *is* the minimal polynomial of α over E^H.

3. Conclude that $\big[E : E^H\big] = |H|$. However, by GT3, we know that $\big[E : E^H\big] = \big|\mathrm{Gal}\big(E/E^H\big)\big|$. Conclude that $H = \mathrm{Gal}\big(E/E^H\big)$.

Proposition. *Let E be a finite Galois extension of F with Galois group G. Then every subgroup of G is itself a Galois group. More specifically, if H is a subgroup of G, then $H = \mathrm{Gal}\big(E/E^H\big)$.*

Problem 4–5. The Galois correspondence. (Let E be a finite Galois extension of F with Galois group G. For any intermediate field L, let $G_L = \mathrm{Gal}(E/L)$.)

4. Rephrase the above proposition as follows. If H is a subgroup of G, then $G_{E^H} = H$.

5. Let L be an intermediate field between F and E. Show that $E^{G_L} = L$, and prove the following theorem. Hint: use GT3.9.

Theorem (Galois Correspondence)**.** *Let E be a finite Galois extension of F with Galois group G. There is an inclusion reversing bijection between (i) the set of subgroups of G and (ii) the set of subfields L of E that contain F. The bijection from (i) to (ii) sends a subgroup H to E^H. The inverse bijection from (ii) to (i), which is also inclusion reversing, sends an intermediate field L to G_L.*

Problem 6–9. Normal subgroups. (Let E be a finite Galois extension of F with Galois group G. Let H be a subgroup of G.)

6. Suppose H is a normal subgroup. Show that if $\beta \in E^H$, then all its G-conjugates are in E^H.

7. Suppose H is a normal subgroup. Show that E^H is Galois over F. Hint: write $E^H = F[\beta]$ for some $\beta \in E$, and consider the splitting field (in E) of the minimal polynomial of β.

8. Suppose E^H is a Galois extension of F. Show that if $\alpha \in E^H$ and $\sigma \in G$ then $\sigma\alpha \in E^H$. Hint: By the minimal polynomial formula, the minimal polynomial $f \in F[X]$ of α has $\sigma\alpha$ as one of its roots.

9. Suppose E^H is a Galois extension of F. Show that the map $G \to \mathrm{Gal}\big(E^H/F\big)$ sending σ to its restriction to E^H is a group homomorphism (and is well-defined). Identify its kernel and image. Hint: For the image, consider GT3.10 (extension property), or just give a counting argument. Conclude that H is a normal subgroup of G. Prove the following:

Theorem (Galois Correspondence, Part 2)**.** *Under the bijections of the previous theorem, normal subgroups of G correspond to Galois extensions of F (contained in E). If H is a normal subgroup of G and E^H is Galois over F, then*

$$\mathrm{Gal}\Big(E^H/F\Big) \cong G/H.$$

Problems 1–4. The top-down approach, where we start with E and form F. (Let E be a field. The automorphisms of E form a group, perhaps an infinite group: see Problem 7 below for an example. Let G be a finite subgroup of the automorphism group of E, and let $F = E^G$ be the field fixed by G.)

1. Let $\alpha \in E$, and let $\alpha_1, \ldots, \alpha_n$ be all the distinct elements of the form $\sigma\alpha$ where $\sigma \in G$. Show that $f = \prod(X - \alpha_i)$ is in $F[X]$, and is the minimal polynomial of α over F. Conclude that E is algebraic and separable over F, and that the minimal polynomial of any element of E splits in E with degree at most $|G|$ and with distinct roots in E.

2. Let L be any finite extension of F contained in E. Since $L = F[\alpha]$ for some $\alpha \in E$, show that

$$[L : F] \leq |G|.$$

Conclude that E itself is a finite extension of F with $[E : F] \leq |G|$.

3. Thus $E = F[\alpha]$ for some $\alpha \in E$. Show that E is the splitting field of the minimal polynomial of α over F. Conclude that E is Galois over F.

4. Show that G is a subgroup of $\mathrm{Gal}(E/F)$, so $|G| \leq [E : F]$. Prove the following:

Theorem. *Let E be a field. Let G be a finite subgroup of the automorphism group of E. Then E is a finite Galois extension of $F = E^G$ with Galois group G.*

Problems 5–7. Numerically Galois extensions. As we will show, if E is a finite extension of F then there are at most $[E : F]$ automorphism of E fixing F. We now develop the point of view that Galois extensions are extensions with as many such automorphisms as possible. (Let E be a finite extension of F. Let G be the group of automorphisms of E which fix F).

5. Show that G is finite. Hint: write $E = F[\alpha_1, \ldots, \alpha_k]$ and consider the set of roots R in E of the minimal polynomials over F of the elements α_i. Show that G injects into the permutations group $\mathcal{S}_R$.

6. Show that $|G|$ divides $[E : F]$, so $|G| \leq [E : F]$. Show that $|G| = [E : F]$ if and only if $[E^G : F] = 1$. Hint: use the above theorem with $F' = E^G$.

Definition. Let E be a finite extension of F. If the number of automorphisms of E fixing F is $[E : F]$ then we say that E is *numerically Galois* over F.

7. Show that E is numerically Galois over F if and only if E is Galois over F.

Problems 8–10. Examples of the top-down approach. (Let K be a field. These problems assume knowledge of fields of fractions.)

Fact. *Suppose R is an integral domain, and that F is a field. Then any injective ring homomorphism $R \to F$ extends uniquely to a homomorphism from the field of fractions of R to F.*

8. Consider the evaluation homomorphism $K[X] \to K[X]$ which sends X to $X - 1$. Show that it is an isomorphism. Show that it extends to an automorphism σ of $K(X)$. Show that if K is infinite, then σ has infinite order in the automorphism group of $K(X)$. Thus automorphism groups can be infinite.

9. Suppose that K contains an element $\zeta \neq 1$ such that $\zeta^3 = 1$. Show that the evaluation homomorphism $K[X] \to K[X]$ which sends X to ζX is an isomorphism. Conclude that it extends to an automorphism τ of $K(X)$ such that τ^3 is the identity map. Let G be the group generated by τ. Show that $K(X)^G = K(X^3)$. Hint: show $X^3 \in K(X)^G$, and that X satisfies a cubic with coefficients in $K(X^3)$.

10. Consider the evaluation homomorphism $K[X] \to K(X)$ which sends X to $1/X$. Show that it extends to an automorphism γ of $K(X)$. Show that γ^2 is the identity map. Let G be the cyclic group generated by γ. Show that $K(X)^G = K\big(X + X^{-1}\big)$. Hint: show $X + X^{-1} \in K(X)^G$, and that X satisfies a quadratic with coefficients in $K\big(X + X^{-1}\big)$.

Cyclotomic extensions.

Definition 1. Roots of $X^n - 1$ in a field E are called *nth roots of unity.* If an nth root of unity has multiplicative order exactly n then it is called a *primitive nth root of unity.*

Definition 2. The *nth cyclotomic extension of a field F* is the splitting field of $X^n - 1$ over F. Let μ_n be the multiplicative group of n roots of unity in the nth cyclotomic extension of F.

Fact. *Let F be a field. Then any finite subgroup of $F^\times$ is cyclic. If C is a cyclic group of order n then there are $\phi(n)$ elements which generate C where $\phi(n)$ is the Euler ϕ function.*

Problems 1–2. Cyclotomic field extensions. (Let F be a field, and n a positive integer. Assume that the characteristic of F does not divide n; for example, this holds if F has characteristic zero.)

1. Show that the nth cyclotomic extension of F is Galois. Show that the nth roots of unity form a cyclic subgroup of $F^\times$ of order n, and that there are $\phi(n)$ primitive nth roots of unity.

2. Let E be the nth cyclotomic extension of F. If $\zeta_n \in E$ is a primitive nth root of unity then $E = F[\zeta_n]$.

Problems 3–9. The Galois group of the cyclotomic extension. Cyclotomic polynomials. (Let F be a field, and n a positive integer. Assume that the characteristic of F does not divide n. Let E be the nth cyclotomic extension of F, and let $\zeta_n \in E$ be a primitive nth root of unity. Let G be the Galois group of E over F.)

3. Let $\sigma \in G$. Show that if $\alpha \in E$ is a primitive nth root of unity, then so is $\sigma\alpha$. Conclude that

$$\sigma\zeta_n = \zeta_n^{m(\sigma)}$$

for some $m(\sigma)$ prime to n.

4. Let σ and $m(\sigma)$ be as above. Show that we can think of $m(\sigma)$ as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$, and if we do so then $m(\sigma)$ is unique. Show also that $\sigma(\alpha) = \alpha^{m(\sigma)}$ for *all* $\alpha \in \mu_n$. Conclude that $m(\sigma)$ is independent of the choice of primitive nth root of unity ζ_n in E.

5. Show that the map $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ defined by the rule $\sigma \mapsto m(\sigma)$ is a homomorphism. Show that this homomorphism is injective. Thus G is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and so $[E : F]$ divides $\phi(n)$, and G is abelian.

6. Let μ'_n be the set of primitive nth roots of unity. Show that $\Phi_F(n) \stackrel{\text{def}}{=} \prod_{\alpha\in\mu'_n}(X-\alpha)$ is a polynomial in $F[x]$ of degree $\phi(n)$, and that the minimal polynomial of ζ_n divides $\Phi_F(n)$. Show that $\Phi_F(n)$ does not depend on the choice of splitting field E of $X^n - 1$. When we write $\Phi(n)$, we mean $\Phi_{\mathbb{Q}}(n)$.

7. Show that $X^n-1 = \prod_{d|n}\Phi_F(d)$ in $F[X]$. Use this recursion to show that if F is any field containing $\mathbb{Q}$, then $\Phi_F(n) = \Phi(n)$ and so $\Phi_F(n) \in \mathbb{Q}[X]$. Use this recursion to calculate as many $\Phi(n)$ as you have patience for.

8. Use Gauss's lemma or the idea of integral elements to show that $\Phi(n)$ is monic with coefficients in $\mathbb{Z}[X]$. If F has characteristic p, use the above recursion to show that $\Phi_F(n)$ is just the polynomial obtained by taking the $\Phi(n) \in \mathbb{Z}[x]$ and reducing the coefficients mod p.

9. Suppose $F = \mathbb{Q}$, and $f \in \mathbb{Q}[X]$ is the minimal (monic) polynomial of ζ_n. Observe that f is a primitive polynomial of $\mathbb{Z}[X]$. Show that if $g \in \mathbb{Z}[X]$ has root ζ_n, then g is a multiple of f in $\mathbb{Z}[X]$. Use the evaluation map $\mathbb{Z}[X] \to \mathbb{Z}[\zeta_n]$ to show that $\mathbb{Z}[\zeta_n]$ is isomorphic to $\mathbb{Z}[X]/\langle f\rangle$. Hint: factor g in $\mathbb{Z}[X]$. Since this gives a factorization in $\mathbb{Q}[X]$, f must be a $\mathbb{Q}[X]$-associate to a primitive irreducible polynomial factor h of g. What does that say about f versus h?

Problem 1–4. The pth reduction map. (Let E be the nth cyclotomic extension of $\mathbb{Q}$, and let μ_n be the nth roots of unity. Let ζ_n be a fixed generator of the cyclic group μ_n, and let $f \in \mathbb{Q}[X]$ be the (monic) minimal polynomial of ζ_n. Let p be a prime not dividing n, and let $\overline{E}$ be the nth cyclotomic extension of $\mathbb{F}_p$. Let $\overline{\mu}_n$ be the nth roots of unity in $\overline{E}$. Let $\pi : \mathbb{Z} \to \mathbb{F}_p$ be the reduction homomorphism. Recall that π extends to a homomorphism $\pi_X : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ which takes a polynomial and reduces its coefficents modulo p.)

1. Show that $\Phi(n) = fg$ for some monic $g \in \mathbb{Q}[X]$, and use Gauss's lemma or integrality to show that, in fact, $f, g \in \mathbb{Z}[X]$. Show that $\Phi_{\mathbb{F}_p}(n) = \overline{f}\overline{g}$ where $\overline{f} = \pi_X f$ and $\overline{g} = \pi_X g$. Let $\overline{\zeta}_n$ be a choice of root of $\overline{f}$ in $\overline{E}$. Show that $\overline{\zeta}_n$ is a primitive nth root of unity in $\overline{\mu}_n$.

2. Let $\overline{\zeta}_n$ be as above, and consider the homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p\left[\overline{\zeta}_n\right]$ obtained by composing the homomorphism $\pi_X : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ with the evaluation map $\mathbb{F}_p[X] \to \mathbb{F}_p\left[\overline{\zeta}_n\right]$ sending X to $\overline{\zeta}_n$. Show that this composition has a kernel containing f, so we have a map $\mathbb{Z}[X]/\langle f\rangle \to \mathbb{F}_p\left[\overline{\zeta}_n\right]$ sending $\overline{X}$ to $\overline{\zeta}_n$. Recall from GT 9.9 that $\mathbb{Z}[\zeta_n]$ is isomorphic to $\mathbb{Z}[X]/\langle f\rangle$. Use this to construct a homomorphism

$$\mathbb{Z}[\zeta_n] \to \mathbb{F}_p\left[\overline{\zeta}_n\right]$$

with $\zeta_n \mapsto \overline{\zeta}_n$. Call this map the *p reduction map*. If $\alpha \in \mathbb{Z}[\zeta_n]$ then we write $\overline{\alpha}$ for its image in $\mathbb{F}_p\left[\overline{\zeta}_n\right]$.

3. Show that this pth reduction map induces an isomorphism $\mu_n \to \overline{\mu}_n$. Show that this isomorphism restricts to give a bijection between roots of f and roots of $\overline{f}$.

4. Suppose $\alpha \in \mu_n$ is a root of f and so, by Problem 3, $\overline{\alpha}$ is a root of $\overline{f}$. Show that $\overline{\alpha}^p$ is a root of $\overline{f}$. Conclude that α^p is a root of f. Hint: use the pth Frobenius automorphism $x \mapsto x^p$.

Problems 5–7. Irreduciblility of the Cyclotomic Polynomial. (Let E be the nth cyclotomic extension of $\mathbb{Q}$. Let $\zeta_n \in E$ be a fixed primitive nth root of unity with minimal polynomial f over $\mathbb{Q}$.)

5. Show that if $\alpha \in E$ is any root of f, and k is any positive integer prime to n, then α^k is a root of f. Hint: use Problem 4.

6. Show that every primitive nth root of unity is a root of f. Show that $f = \Phi(n)$. Prove the following theorem and corollaries.

Theorem. *The nth cyclotomic polynomial $\Phi(n)$ is irreducible in $\mathbb{Q}[X]$.*

Corollary 1. *The nth cyclotomic extension E of $\mathbb{Q}$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Hence $[E : \mathbb{Q}] = \phi(n)$.*

Corollary 2. *Suppose E is the qth cyclotomic extension of $\mathbb{Q}$ where q is a prime. If L is a field intermediate between $\mathbb{Q}$ and E, then $[L : \mathbb{Q}]$ divides $q - 1$. For every divisor d of $q - 1$ there is a unique intermediate extension L_d with $[L_d : \mathbb{Q}] = d$. The field L_d is Galois over $\mathbb{Q}$ with Galois group cyclic of order d. For such divisors d, d', the field L_d is contained in $L_{d'}$ if and only if $d|d'$.*

7. Suppose that q is an odd prime. Show that the qth cyclotomic extension of $\mathbb{Q}$ contains a unique quadratic (degree 2) extension L of $\mathbb{Q}$. Our next goal will be to describe this quadratic extension.

Problem 8–9. Quadratic extensions and square roots. (Let E be a quadratic (degree 2) extension of a field F. Assume that the characteristic of F is not 2)

8. Show that E is Galois over F. If $\sigma \neq \mathrm{id}$ in the Galois group, and $\beta \in E$ then $\sigma\beta$ is written $\overline{\beta}$.

9. Suppose $\beta \in E$ not in F. Let $\delta = \beta - \overline{\beta}$. Show that $\overline{\delta} = -\delta$. Conclude that the minimal polynomial of δ is $(X - \delta)(X + \delta) = X^2 - \delta^2$. In particular $d = \delta^2 \in F$, and $E = F[\delta]$. We write δ as $\sqrt{d}$ (although, really d has two square roots in E, which differ by a sign), and E as $F[\sqrt{d}]$. Show that $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$ for any $a, b \in F$. If $F = \mathbb{Q}$ show further that $E = F[\sqrt{d}]$ where d can be chosen to be a square-free integer $d \neq 1$, and such d is unique (those with $d > 0$ are called *real quadratic fields* and those with $d < 0$ are called *imaginary quadratic fields*).

Generators of quadratic subfields. (Let E be a finite Galois extension of F where F is a field of characteristic not equal to 2. Suppose G is the Galois group, and suppose H is a subgroup of index 2 in G. So E^H is a quadratic extension of F.)

1. We wish to build on the idea of GT 10.9 to find a $d \in F$ such that $E^H = F[\sqrt{d}]$. We assume we have elements of E (such as generators). But to use GT 10.9 we need to find a β in the subfield E^H. We start with the idea of averaging. If $\alpha \in E$ then consider the average of its H-conjugates

$$\frac{1}{|H|} \sum_{\sigma \in H} \sigma\alpha.$$

Since dividing by $|H|$ creates problems in finite characteristic, we just consider $\beta = \sum_{\sigma \in H} \sigma\alpha$. Show that $\beta \in E^H$. (Note: this "trace" idea works for any subgroup of H, not just index 2 subgroups).

2. Let α, β be as above. Since E^H is quadratic, we have a conjugate $\overline{\beta} \in E^H$. Show that $\overline{\beta}$ is $\tau\beta$ where $\tau \in G$ is any element not in H. Show that

$$\overline{\beta} = \tau \sum_{\gamma \in H} \gamma\alpha = \sum_{\gamma \in H} \tau\gamma\alpha = \sum_{\sigma \in \tau H} \sigma\alpha = \sum_{\sigma \notin H} \sigma\alpha.$$

As in GT 10.9, we wish to consider $\delta = \beta - \overline{\beta}$, which satisfies $\overline{\delta} = -\delta$. Observe that

$$\delta = \beta - \overline{\beta} = \sum_{\sigma \in H} \sigma\alpha - \sum_{\sigma \notin H} \sigma\alpha = \sum_{\sigma \in G} \chi(\sigma)\sigma\alpha$$

where $\chi : G \to \{\pm 1\}$ is as defined as follows. (Note: in our sums, think of ± 1 as elements of F).

Definition. The *quadratic character* $\chi : G \to \{\pm 1\}$ associated to H is the map defined by the rule $\chi(\sigma) = 1$ if $\sigma \in H$ and $\chi(\sigma) = -1$ if $\sigma \notin H$.

3. Show that the quadratic character χ is a surjective group homomorphism.

4. If $\delta \neq 0$, then δ has minimal polynomial $X^2 - d$ where $d = \delta^2$. Show (whether or not $\delta = 0$) that

$$d = \sum_{\sigma, \tau \in G} \chi(\sigma\tau)(\sigma\alpha)(\tau\alpha).$$

Conclude that if $d \neq 0$ then $E^H = F[\sqrt{d}]$.

5. Specialize to the situation where $F = \mathbb{Q}$, where E is the qth cyclotomic extension of $\mathbb{Q}$ for q an odd prime, and where $\alpha = \zeta$ is a primitive qth root of unity. Identify the Galois group G with $(\mathbb{Z}/q\mathbb{Z})^\times$. Show that the unique subgroup H of index two is the set of squares in $(\mathbb{Z}/q\mathbb{Z})^\times$ (the set of quadratic residues). Under this identification with G show that

$$d = \sum_{\sigma, \tau \in G} \chi(\sigma\tau)(\sigma\zeta)(\tau\zeta) = \sum_{k,l \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right) \zeta^k \zeta^l = \sum_{k,l \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right) \zeta^{k+l}.$$

Here $\left(\frac{a}{q}\right)$ is the Legendre symbol: it is $+1$ if a is a nonzero square mod q and -1 if a is not a square mod q. Now prove the following lemma (later we will calculate d and find that it is not zero):

Lemma. *Let E be the qth cyclotomic extension of $\mathbb{Q}$ where q is an odd prime. Let ζ be a primitive qth root of unity. Let*

$$d \stackrel{\text{def}}{=} \sum_{k,l \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right) \zeta^{k+l}.$$

Then d is in $\mathbb{Q}$. Furthermore, if $d \neq 0$ then $\mathbb{Q}[\sqrt{d}]$ is the unique quadratic extension of $\mathbb{Q}$ contained in E.

Problems 1–3. The quadratic subfield of $\mathbb{Q}[\zeta_q]$. (Let E be the qth cyclotomic extension of $\mathbb{Q}$ where q is an odd prime. Let $\zeta = \zeta_q$ in E be a primitive q root of unity.)

1. Our goal is to calculate the following d, known to be an element of $\mathbb{Q}$:

$$d = \sum_{k,l \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right) \zeta^{k+l} = \sum_{m=0}^{q-1} A_m \zeta^m \qquad \text{where} \qquad A_m = \sum_{k \neq m} \left(\frac{k(m-k)}{q}\right).$$

In the formula for A_m, the terms vary over $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ with $k \neq m$ in $\mathbb{Z}/q\mathbb{Z}$. Justify the formula for A_m, and show that

$$A_0 = \sum_{k \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{-k^2}{q}\right) = \sum_{k \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{-1}{q}\right) = (q-1)\left(\frac{-1}{q}\right).$$

2. Now assume $m \neq 0$. Show that for each $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ with $k \neq m$ there is a unique $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $m - k = rk$. Show that this yields every r except $r = -1$. Conclude that

$$A_m = \sum_{k \neq m} \left(\frac{k(m-k)}{q}\right) = \sum_{r \neq -1} \left(\frac{k^2 r}{q}\right) = \sum_{r \neq -1} \left(\frac{r}{q}\right) = -\left(\frac{-1}{q}\right) + \sum_{r=1}^{q-1} \left(\frac{r}{q}\right) = -\left(\frac{-1}{q}\right).$$

3. What is the qth cyclotomic polynomial $\Phi(q)$? Use the fact that ζ is a root of $\Phi(q)$ to show that

$$\zeta + \zeta^2 + \ldots + \zeta^{q-1} = -1.$$

Show that $d = \left(\frac{-1}{q}\right) q$. Conclude the following:

Theorem. *Let E be the qth cyclotomic extension of $\mathbb{Q}$ where q is an odd prime. Define $*q = \left(\frac{-1}{q}\right) q$. Then $\mathbb{Q}\left[\sqrt{*q}\right]$ is the unique quadratic extension of $\mathbb{Q}$ contained in E. Furthermore, $\sqrt{*q}$ is in the ring $\mathbb{Z}[\zeta]$ where ζ is a primitive qth root of unity.*

Problems 4–8. Proof of Quadratic Reciprocity. (Let E be the qth cyclotomic extension where q is an odd prime, and let $p \neq q$ be another odd prime. Let ζ be a primitive qth root of unity. Let G be the Galois group of E over $\mathbb{Q}$ which we identify with $(\mathbb{Z}/q\mathbb{Z})^\times$. Let H be the subgroup of index 2 which we identify with the squares or quadratic residues. Let $\alpha \mapsto \overline{\alpha}$ be the pth reduction map $\mathbb{Z}[\zeta] \to \mathbb{F}_p\left[\overline{\zeta}\right]$ defined in GT 10.)

4. The element $\sigma_p \in G$ that is identified with $p \in (\mathbb{Z}/q\mathbb{Z})^\times$ is called the *pth Frobenius element*. It has the property that $\sigma_p(\alpha) = \alpha^p$ for all roots of unity $\alpha \in \mu_q$. Of course $\sigma_p(\alpha) = \alpha^p$ does not hold for all $\alpha \in E$. However, show that if $\alpha \in \mathbb{Z}[\zeta]$ then $\overline{\sigma_p \alpha} = \overline{\alpha}^p$.

5. Observe that $\sigma_p \in H$ if and only if p is a square mod q. Show that if $\alpha \in \mathbb{Z}[\zeta]$ is in E^H and p is a square mod q then $\overline{\alpha} \in \mathbb{F}_p$. Conclude that if p is a square mod q, then $*q$ is a square mod p.

6. Show that if p is not a square mod q then $\sigma_p \sqrt{*q} = -\sqrt{*q}$. Show that $\overline{\sqrt{*q}}$ is not in $\mathbb{F}_p$. Conclude that $*q$ is not a square mod p.

7. Show the following equation between Legendre symbols.

$$\left(\frac{p}{q}\right) = \left(\frac{*q}{p}\right).$$

8. Show that -1 is a square mod q if and only if $q \equiv 1 \bmod 4$. Use this to prove the following.

Theorem (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

Ruler and compass constructions.

Definition 1. Let F be a subfield of $\mathbb{R}$. A point (a, b) of $\mathbb{R}^2$ is called *F-rational* if $a, b \in F$. A line of $\mathbb{R}^2$ is said to be *generated* by two distinct points (a, b) and (c, d) if it contains the two points. A circle of $\mathbb{R}^2$ is said to be *generated* by $(a, b), (c, d)$ and (e, f) if has center (a, b) and radius equal to the distance from (c, d) to (e, f). (Here we assume that (c, d) and (e, f) are distinct).

Definition 2. Let S be a set of points of $\mathbb{R}^2$. Let $RC^1(S)$ be the set consisting of S together with any point (a, b) which is the point of intersection of (distinct) curves C_1 and C_2 where C_i is either a line generated by two points of S or a circle generated by three points of S.

Let $RC^2(S)$ be $RC^1(RC^1(S))$, let $RC^{n+1} = RC^1(RC^n(S))$. Let $RC(S)$ be the union of the sets $RC^n(S)$.

Definition 3. A point is said to be *constructible* if it is in $RC(S)$ where S is the set $\{(0, 0), (1, 0)\}$. A line generated by constructible points is said to be a *constructible line*. A circle generated by constructible points is said to be a *constructible circle*. Let $\mathbb{E}$ be the set of all $a \in \mathbb{R}$ that occur as a coordinate of a constructible point.

Problems 1–4. Quadratic towers associated to constructible points. (Let F be a subfield of $\mathbb{R}$.)

1. Show that a line can be generated by two F-rational points if and only if it is the solution set of $ax + by + c = 0$ with $a, b, c \in F$ and with a and b not both zero. Suppose ℓ_1 and ℓ_2 are two distinct nonparallel lines, each generated by F-rational points. Show that the intersection of ℓ_1 and ℓ_2 is F-rational. Show that if a circle can be generated by three F-rational points, then it is the solution set of an equation of the form $x^2 + y^2 + ax + by + c = 0$ where $a, b, c \in F$.

2. Suppose that $a, b, c, a', b', c' \in F$. Suppose a, b are not both zero. Show that there is a quadratic extension $E \subseteq \mathbb{R}$ of F such that all $x, y \in \mathbb{R}$ with

$$ax + by + c = 0 \qquad x^2 + y^2 + a'x + b'y + c' = 0$$

have the property that $x, y \in E$.

Suppose that $a, b, c, a', b', c' \in F$ where $(a, b, c) \neq (a', b', c')$. Suppose $x, y \in \mathbb{R}$ are such that both

$$x^2 + y^2 + a'x + by + c = 0, \quad \text{and} \quad x^2 + y^2 + a'x + b'y + c' = 0.$$

Show that $(a - a')x + (b - b')y = (c - c')$ also holds, and that either $a - a'$ or $b - b'$ is not zero. Conclude, as above, that there is a quadratic extension $E \subseteq \mathbb{R}$ of F such that $x, y \in E$.

3. Prove the following proposition and corollary.

Proposition. *If (a, b) is constructible, then then there is a sequence F_i of subfields of $\mathbb{R}$ such that*

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{n-1} \subsetneq F_n,$$

such that each $[F_{i+1} : F_i] = 2$, and such that $a, b \in F_n$.

Corollary. *If $a \in \mathbb{E}$ then a is algebraic and $[\mathbb{Q}[a] : \mathbb{Q}]$ is a power of two.*

4. Show that $\pi^{1/2}$ and $2^{1/3}$ are not in $\mathbb{E}$. Explain why it is impossible to duplicate the cube or square the circle. (The problem of duplicating the unit cube, say, is to find two points P and Q such that PQ has length a, where a is the length of the side of a cube with volume 2. The problem of squaring the unit circle, say, is to find P and Q such that PQ has length a, where a is the length of the side of a square with area equal to that of the unit circle.)

Problems 1–9. The fields $\mathbb{E}$ and $\mathbb{E}[i]$.

1. Let P and Q be constructible points. Show that the perpendicular bisector to the segment PQ is constructible. Conclude that the midpoint of the segment PQ is constructible.

2. Assume that P is a constructible point and that ℓ is a constructible line. Show that the line perpendicular to ℓ containing P is constructible. Do two cases (i) $P \in \ell$ and (ii) $P \notin \ell$.

3. Show that the x and y-axes are constructible lines. Show that if (a, b) is constructible then so are $(a, 0), (0, b)$ and $(b, 0)$. Show that (a, b) is constructible if and only if $a, b \in \mathbb{E}$.

4. Show that if $a, b \in \mathbb{E}$ then so are $a + b$ and $-a$. Conclude that $\mathbb{E}$ is an additive subgroup of $\mathbb{R}$.

5. Suppose that $a, b \in \mathbb{E}$ with $a \neq 0$. Show that (b, ab) and $(1/a, 1)$ are constructible. Conclude that $\mathbb{E}$ is an intermediate field between $\mathbb{Q}$ and $\mathbb{R}$. Hint: consider the line generated by $(0, 0)$ and $(1, a)$, and its intersection with $x = b$ and $y = 1$.

6. Show that if $a > 0$ is in $\mathbb{E}$ then $a^{1/2} \in \mathbb{E}$. Conclude that the field $\mathbb{E}$ is closed under square roots of nonnegative elements. Hint: look at the circle with center $(0, 0)$ and containing $\big(0, (a + 1)/2\big)$. Where does this circle intersect the line $x = (a - 1)/2$?

7. Show that (a, b) is constructible if and only if $a+bi \in \mathbb{E}[i]$. So we can think of $\mathbb{E}[i]$ as the subfield of $\mathbb{C}$ consisting of constructible points. In other words, complex numbers representing constructible points forms a subfield of $\mathbb{C}$.

8. Show that if $\alpha \in \mathbb{E}[i]$ then $\pm\alpha^{1/2} \in \mathbb{E}[i]$. Hint: you may need to bisect an angle.

9. Prove the following. Hint: use the proposition of GT 13.

Theorem. *Suppose $\alpha = a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$. Then (a, b) is constructible if and only if there is a sequence of subfields of $\mathbb{C}$*

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{n-1} \subsetneq F_n,$$

such that each $[F_{i+1} : F_i] = 2$, and such that $\alpha \in F_n$.

Corollary. *If $\alpha \in \mathbb{E}[i]$ then α is algebraic and the degree $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ is a power of two.*

Problems 10–13. Polygons and trisections.

10. Show that a primitive nth root of unity ζ_n is in $\mathbb{E}[i]$ if and only if $\phi(n)$ is a power of 2. Conclude that the pentagon and the 17-gon are constructible (the first was known to the ancients, and the last is a result of Gauss). Hint: use the first corollary of GT 10. Show that if an Abelian group has order a power of two, then it has a (normal) subgroup of order 2. (When we say that an n-gon is “constructible” we mean that the all the vertices of some regular n-gon are constructible.)

11. Show that an n-gon is constructible if and only if $\zeta_n \in \mathbb{E}[i]$. Hint: Suppose you have constructed a regular n-gon. From the vertices you can construct the center. You can subtract all the vertices by the center and divide a pair of resulting vertices to obtain a primitive nth root of unity.

12. Show that there are constructible angles whose trisection is not constructible. Conclude that not all angles can be trisected with ruler and compass. Hint: consider a primitive 6th root of unity and a primitive 18th root of unity. (An angle is constructible means that the vertex and at least one point on each side is constructible).

13. Identify n such that $\phi(n)$ is a power of two. Do so in terms of powers of two and Fermat primes (primes of the form $2^n + 1$). Note: this requires some basic knowledge of the Euler phi function.

Galois theory of finite fields.

Fact. *Every finite field has characteristic p for some prime p, and has a subfield canonically isomorphic to $\mathbb{F}_p$. So we regard every finite field of characteristic p as a finite extension of $\mathbb{F}_p$.*

1. Show that if F is a field with q elements, then every element of $F^\times$ is a root of $X^{q-1} - 1$. Show that every element of F is a root of $X^q - X$. Factor $X^q - X$ in $F[X]$.

2. Let F be a finite field with q elements, and let E be a finite extension of degree n. Show that E has q^n elements. Show that E is the splitting field of $X^{q^n} - X$ over F. Conclude that E is Galois over F with a Galois group of size n.

3. Conclude from the above that if E is a finite field of characteristic p, then $|E|$ is p^n for some n, and E is Galois over $\mathbb{F}_p$. Furthermore $x^{p^n} = x$ for all $x \in E$.

Definition. Suppose that F is a field of characteristic p. Let q be a power of p. Then the qth power *Frobenius map* $\mathrm{Fr}_q \colon F \to F$ is the function $x \mapsto x^q$.

4. Let F be a field of characteristic $p > 0$, and let q be a power of p. Show that Fr_q is an automorphism of F. Show that $(\mathrm{Fr}_q)^k = \mathrm{Fr}_{q^k}$ in the automorphism group of F. Show that at most q elements of F are fixed by Fr_q, and these element form a subfield of F.

5. Prove the following theorem and corollary.

Theorem. *Let F be a finite field with q elements, and let E be a finite extension of degree n. Then E is Galois over F, and Fr_q is an element of $\mathrm{Gal}(E/F)$. Further, $\mathrm{Gal}(E/F)$ is cyclic of order n with generator Fr_q.*

Corollary. *Let F be a finite field with q elements and let E be a degree n extension. For all positive divisors k of n there is a unique field L_k intermediate between F and E of size q^k.*

6. Let F be a finite field with q elements. For each $n \geq 1$, let E_n be the splitting field of $f = X^{q^n} - X$ over F. Show that $f' = -1$ and that the extension E has at least q^n elements. Consider the Frobenius automorphism Fr_{q^n} of E_n, and let E' be the elements fixed by Fr_{q^n}. Show that E' is a subfield containing F and that E' is the set of roots of $X^{q^n} - X$ in E_n. Conclude that $E_n = E'$, and that E has exactly q^n elements, and conclude the following:

Theorem. *Let F be a field with q elements. For each $n \geq 1$ there is an extension of F of degree n. This extension is the splitting field of $X^{q^n} - X$ over F, and is unique up to isomorphism (and the isomorphisms can be required to fix F).*

Corollary. *Let p^n be a power of a prime. There is a field with p^n elements, and any two such fields are isomorphic.*

7. Prove the following:

Theorem. *Let E be an algebraic closure of $\mathbb{F}_p$. For each power p^n, there is a unique subfield of E of order p^n. These are all the finite subfields of E. If L_1, L_2 are finite subfields of E then $L_1 \subseteq L_2$ if and only if $|L_2|$ is a power of $|L_1|$.*

8. Let p be a prime. Show that E is a field with p^n elements if and only if it is a $p^n - 1$ cyclotomic extension of $\mathbb{F}_p$. Let $|E| = p^n$. Show that every root of the cyclotomic polynomial $\Phi_{\mathbb{F}_p}(p^n - 1)$ generates the group $E^\times$. Show that $\Phi_{\mathbb{F}_p}(p^n - 1)$ factors in $\mathbb{F}_p[X]$ into irreducible factors of degree n, and that if α is a root of any one of these, then $E = \mathbb{F}_p[\alpha]$.

Problems 1–5. The fundamental theorem of algebra. (We will use four facts from outside Galois theory. Two are from analysis, and two are from finite group theory. Fact 1 follows from the intermediate value theorem. The geometric description of multiplication in $\mathbb{C}$ then yields Fact 2. Problem 8 gives another argument for Fact 2. Fact 3 is a standard result of group theory called the first Sylow theorem. Fact 4 is also a standard fact in group theory, and so can be taken as given; however, a short proof is outlined in Problem 3.)

Fact 1. *Every polynomial $f \in \mathbb{R}[X]$ of odd degree has a real root. If $a > 0$ then $x^2 = a$ has solutions in $\mathbb{R}$.*

Fact 2. *If $a \in \mathbb{C}$ then $x^2 = a$ has a solution in $\mathbb{C}$.*

Fact 3. *Let G be a finite group, p a prime, and p^n the largest power of p dividing $|G|$. Then G has a subgroup of order p^n (called a p-*Sylow subgroup*).*

Fact 4. *Let G be a group of order 2^n, $n \geq 1$. Then G has a subgroup of index 2.*

1. Show that there are no finite extensions of $\mathbb{R}$ of odd degree greater than 1. Show that there are no extensions of $\mathbb{C}$ of degree two.

2. Let E be a finite Galois extension of $\mathbb{R}$ with Galois group G. Show that $|G|$ is a power of 2. Hint: look at $[E^H : \mathbb{R}]$ where H is a 2-Sylow subgroup of G.

3. (Optional) Prove fact 4. Hint: induction on n. The center of G is non-trivial (look at orbits under conjugation). Show that the center has an element σ of order 2. Use the group $G/\langle\sigma\rangle$.

4. Show that $\mathbb{C}$ has no proper finite extensions. Then prove the following theorem. Hint: let E be a Galois extension of $\mathbb{R}$ containing the given extension of $\mathbb{C}$. Use Fact 4 on $\mathrm{Gal}(E/\mathbb{C})$.

Theorem (Fundamental theorem of algebra)**.** *The field $\mathbb{C}$ is algebraically closed. The field $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. All irreducible polynomials in $\mathbb{R}[x]$ are either linear, or quadratic with distinct conjugate roots in $\mathbb{C}$.*

Problems 5–9 (Optional). A general form of the fundamental theorem of algebra. (Let R be a real closed field as defined below. Let C be the splitting field of $X^2 + 1$ over R. Let i be a root of $X^2 + 1$ in C, so $C = R[i]$. If $a, b \in R$, then define the norm of $\alpha = a + bi \in C$ to be $\alpha\overline{\alpha} = a^2 + b^2$.)

Definition. Let R be an ordered field. We say that R is a *real closed field* if (i) every odd degree polynomial $f \in R[X]$ has a root in R. and (ii) every positive element has a square root in R.

5. Recall that an ordered field L has characteristic zero, that $1 \in L$ is positive, and that the square of any element of L is nonnegative. Conclude that $X^2 + 1$ is irreducible in $L[X]$.

6. If $a, b \in R$, show that the norm of $a + bi$ is nonnegative, and zero only if $a = b = 0$. Show that the norm is a multiplicative map $C \to R$.

7. Suppose $u = a + bi$ has norm 1 and $b \geq 0$. Show that $-1 \leq a \leq 1$. Derive, or at least verify, that

$$\sqrt{\frac{1+a}{2}} + i\sqrt{\frac{1-a}{2}}$$

yields a formula for a square root of u. (Where the square roots are taken as nonnegative roots in R). Hint: to derive the formula, start with the fact that the square root must also have norm 1.

8. Show that every element of C has a square root in C.

9. Generalize the fundamental theorem of algebra to C and R using Problems 1, 2, and 4 as a model.