Chapter 9

Dave

May 2, 2015

1 Finite and Algebraic Extensions

1. Let $E = K(a_1, a_2, \ldots a_n)$, then $E \subset F(a_1, \ldots a_n)$ since $K \subset F$, and it is clear that $F \subset F(a_1, \ldots a_n)$, so $F(a_1, \ldots a_n)$ is an algebraic extension of F containing F and E so $E \circ F \subset F(a_1, \ldots a_n)$ so $E \circ F$ is algebraic.

2. By part a, $E \circ F$ is an algebraic extension of the algebraic extension F, so it follows from Proposition 9.1b that $E \circ F$ is algebraic.

3. As noted in Exercise 1, $E \circ F \subset F(a_1, \ldots a_n)$, which has dimension at most $\dim_K(K(a_1, \ldots a_n)) = \dim_K(E)$.

4. 4

2 Splitting Fields

1. If the degree of f is one then f is already factored into linear factors over $K[x]$. Suppose there exists an extension field L of K for any polynomial g of degree less than n such that g factors into linear factors over $L[x]$. Then if f has degree n, then let α be a root of f that is not in K, and it follows that $f(x) = (x - \alpha)g(x)$, where g has degree $n - 1$, so by the induction hypothesis g factors into linear factors over some extension of K, so f does too.

2. Verified!

3. (a) For each $n \in \mathbb{N}$, only finitely many polynomials of degree n exist over a finite field K, so since infinitely many polynomials are irreducible, there must exist irreducible polynomials of arbitrarily large degree.

   (b) By Proposition 9.2.1, every polynomial over K has a splitting field, so polynomials of arbitrarily large degree induce splitting fields of arbitrarily large degree.

(c) Let α be an element by which we're extending K, and let f be the minimal polynomial for α, of degree n. Then $K(\alpha) \subset K \cup (\cup(\sum_{i=0}^{n} k_i x^i))$ over all $k_i \in K$. Both sets in the right-hand union are finite, and the union of finite sets is finite, so $K(\alpha)$ is finite. Inductively, any finite-dimensional extension of a finite field is finite.

3 The Derivative and Multiple Roots

1. Let $f(x) = \sum_n k_n x^n, g(x) = \sum_n l_n x^n$, then $D(f(x)+g(x)) = D(\sum_n k_n x^n + \sum_n l_n x^n) = D(\sum_n (k_n + l_n) x^n) = \sum_n n(k_n + l_n) x^{n-1} = \sum_n n k_n x^{n-1} + \sum_n n l_n x^{n-1} = D(f(x)) + D(g(x))$.

   And $D(f(x)g(x)) = D(\sum_i \sum_j (l_i k_j) x^{i+j}) = \sum_i \sum_j (l_i k_j (i+j)) x^{i+j-1} = \sum_i \sum_j (l_i k_j i) x^{i+j-1} + \sum_i \sum_j (l_i k_j j) x^{i+j-1} = fDg + gDf$.

2. (a) f is constant $\leftrightarrow \exists k \in K : f(x) = k = kx^0 \leftrightarrow Df(x) = 0k = 0$. The "only if" part of that last $\leftrightarrow$ holds only in a field of characteristic 0.

   (b) $f(x) = g(x^p) \leftrightarrow p$ divides the exponent of every x in $f \leftrightarrow p$ divides the coefficient of every x in $Df \leftrightarrow Df = 0$.

3. a is a multiple root of $f \leftrightarrow (x-a)$ divides $g \leftrightarrow g(a) = 0 \leftrightarrow Df(a) = D((x-a)g)(a) = D(x-a)(a)g(a) + (x-a)Dg(a) = 0 + 0 = 0$, since the second term is always 0.

4. The quotient and remainder upon dividing one element of $K[x]$ by another are both elements of $K[x]$, regardless of what extension field of $K[x]$ they are being considered as elements of. Since iterative quotient-remainder calculation is all there is to the GCD formula, it follows that the GCD of two elements of $K[x]$ is the same whether the elements are regarded as elements of $K[x]$ or $L[x]$ for any extension L.

5. By exercise 9.3.3, $(x-a)$ is a common divisor of f and Df.

6. (a) If Df isn't 0 then by the previous exercise f and Df have a common factor of positive degree, so f can't be irreducible since the degree of Df is at most one less than the degree of f, so this common factor has degree less than f. Thus, if f is irreducible and has a multiple root, then $Df = 0$.

   (b) f has a multiple root $\rightarrow Df = 0$ by part a $\rightarrow f$ is constant by Exercise 9.3.2. But a constant polynomial has only simple roots, so it cannot be the case that f has a multiple root.

7. The binomial coefficient $\binom{p}{k}$ is divisible by p whenever $0 < k < p$, so $(x+a)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = x^p + (\sum_{k=1}^{p-1} \binom{p}{k} x^k) + a^p = x^p + (\sum_{k=1}^{p-1} 0x^k) + a^p = x^p + a^p$.

4 Splitting Fields and Automorphisms

1. (a) If $f \in H$ fixes $a, b \in L$, then $f(a+b) = f(a) + f(b) = a + b$, and $f(ab) = f(a)f(b) = ab$, so f fixes $a+b$ and ab so $\mathrm{Fix}(H)$ is a subfield of L.
   (b) H fixes the points fixed by H, so since it is a group it is a subgroup of the group of permutations fixing the points it fixes, aka $\mathrm{Aut}_{\mathrm{Fix}(H)}(L)$.
   (c) The automorphisms that fix K fix K, so K is a subset of the points fixed by the set of automorphisms that fix K, aka $\mathrm{Fix}(\mathrm{Aut}_K(L))$.

2. (a) Any permutation that fixes H_2 must also fix H_1, since $H_1 \subset H_2$, so $H_1^\circ \supset H_2^\circ$.
   (b) Any automorphism that fixes K_2 must also fix K_1, since $K_1 \subset K_2$, so $K_1' \supset K_2'$.

3. (a) $(H^\circ)'^\circ = \mathrm{Fix}(\mathrm{Aut}_{\mathrm{Fix}(H)}(L))$, which is the set fixed by the automorphisms that fix $\mathrm{Fix}(H)$, namely $\mathrm{Fix}(H)$, so $(H^\circ)'^\circ = H^\circ$.
   (b) $(K')^{\circ\prime} = \mathrm{Aut}_{\mathrm{Fix}(\mathrm{Aut}_K(L))}(L)$, so the automorphisms on L that fix the set by the automorphisms on L that fix K is precisely the set of automorphisms that fix K, so $(K')^{\circ\prime} = K'$.

4. Since f is separable in $K[x]$, it has only simple roots in any extension of $K[x]$, so in the extension $M[x]$ of $K[x]$ it has only simple roots, so it is simple over M.

5 The Galois Correspondence

1. The union of the finite-dimensional intermediate extensions M is a subset of L since it is a union of subsets of L, and for any $x \in L$, we have $K(x)$ a finite-dimensional algebraic extension of K, since L is algebraic, so L is a subset of the union of finite-dimensional intermediate extensions.

2. (a) $p(x)$ splits in $A(\alpha)$ since it splits in $K(\alpha)$ and $K \subset A$, so $A(\alpha) = A \circ B$ is the splitting field of p over A, so $A \circ B$ is Galois.
   (b) Restriction is a homomorphism. Every $\tau \in \mathrm{Aut}_A(A \circ B)$ is the identity on A, so if $\tau_{|B}$ is the identity then τ is the identity on A and B, so τ is the identity on $A \circ B$, so $\tau \to \tau_B$ is injective.
   (c) Indeed.

6 Symmetric Functions

1. (a) Sums and scalar products of polynomials of total degree d also have total degree d, and the number of total polynomials of degree d in n variables is the number of sets of n nonnegative integers whose sum is d, which is finite, so $K_d[x_1, \ldots x_n]$ is a finite-dimensional subspace of $K[x_1, \ldots x_n]$.

(b) I got a recursive formula for it, at least. Let $f(n,d)$ be the number of polynomials in n variables of degree d. Then $f(n,0) = f(1,d) = 1$ for all n, d, since the unique monic polynomial in n variables of total degree 0 is $f(x_1, \dots x_n) = 1$ and the unique monic polynomial of degree d in one variable is $f(x) = x^d$. And $f(n,d) = \sum_{i=0}^{d} f(n-1,i)$, because to get all the polynomials of degree d in n variables, you take all the polynomials of degree $\leq d$ in fewer than n variables and multiply the ones of total degree k by x^{d-k}.

(c) $\sum_i a_i x^{\alpha_i} \to (\sum_{|\alpha_j|=1} a_j x^{\alpha_j}, \sum_{|\alpha_j|=2} a_j x^{\alpha_j}, \dots \sum_{|\alpha_j|=d} a_j x^{\alpha_j}, \dots)$ is an isomorphism between the two groups.

2. (a) Let $f, g \in K[x]$, then $\sigma(f+g)(x_1, \dots x_n) = (f+g)(x_{\sigma(1)}, \dots x_{\sigma(n)}) = f(x_{\sigma(1)}, \dots x_{\sigma(n)}) + g(x_{\sigma(1)}, \dots x_{\sigma(n)}) = \sigma(f)(x_1, \dots x_n) + \sigma(g)(x_1, \dots x_n)$. And $\sigma(fg)(x_1, \dots x_n) = (fg)(x_{\sigma(1)}, \dots x_{\sigma(n)}) = f(x_{\sigma(1)}, \dots x_{\sigma(n)}) g(x_{\sigma(1)}, \dots x_{\sigma(n)}) = (\sigma f(x_1, \dots x_n))(\sigma g(x_1, \dots x_n))$. Similar proofs hold for $K(x)$, so S_n acts on $K[x]$ and $K(x)$ by ring/field automorphisms.

(b) Let $f, g \in K^S[x_1, \dots x_n]$, $\sigma \in S_n$, then $\sigma(f+g) = \sigma(f) + \sigma(g) = f + g$, and $\sigma(fg) = \sigma(f)\sigma(g) = fg$, so $K^S[x_1, \dots x_n]$ is a subring of $K[x_1, \dots x_n]$, and similarly $K^S(x_1, \dots x_n)$ is a subring of $K(x_1, \dots x_n)$.

(c) If f and g are symmetric, then for $\sigma \in S_n$, $\sigma(f/g) = \sigma(f)/\sigma(g) = f/g$, so f/g is symmetric. On the other hand, let f/g be a symmetric rational function, then $\frac{f}{g} + \sigma(\frac{f}{g}) = \frac{f\sigma(g) + g\sigma(f)}{g\sigma(g)} = 2\frac{f}{g}$, so equating denominators we find that $\sigma(g)$ divides $f\sigma(g) + g\sigma(f)$, so in particular it divides $g\sigma(f)$, but it can't divide $\sigma(f)$ or else $\sigma(f/g) = f/g$ would be reducible as a fraction. So $\sigma(g)$ divides g, and it follows that $\sigma(g) = g$ since σ is just a permutation so it can't be multiplying g by any non-identity element of K. It follows that $\sigma(f) = f$, so f/g is symmetric $\leftrightarrow$ f and g are symmetric, so the field of symmetric rational polynomials is the field of fractions of the ring of symmetric polynomials.

3. (a) Let $x = \prod_i x_i^{a_i} \in K_d[x_1, \dots x_n]$, then $\sum_i a_i = d$ so $\sum_i a_{\sigma(i)} = d$ for any $\sigma \in S_n$, so $\sigma(x) \in K_d[x_1, \dots x_n]$ so $K_d[x_1, \dots x_n]$ is invariant under the action of S_n.

(b) Sums and scalar products of monomials of total degree d have total degree d, so $K_d^S[x_1, \dots x_n]$ is a vector subspace of $K^S[x_1, \dots x_n]$.

(c) Same proof as exercise 1c, just use $K^S[x_1, \dots x_n]$ instead of $K[x_1, \dots x_n]$.

4. If $n = 1$, then the expression simplifies to 1=1, which follows from the reflexive property of equality. So suppose $\sum_{k=0}^{n-1}(-1)^k \epsilon_k x^{n-k} = \prod_{k=0}^{n-1}(x - x_k)$. Then $\prod_{k=0}^{n}(x - x_k) = (x - x_n)\sum_{k=0}^{n-1}(-1)^k \epsilon_k x^{n-k} = x\sum_{k=0}^{n-1}(-1)^k \epsilon_k x^{n-k} - x_n \sum_{k=0}^{n-1}(-1)^k \epsilon_k x^{n-k} = \sum_{k=0}^{n}(-1)^k(\epsilon_k(x_1, \dots x_{n-1}) + x_n \epsilon_{k-1}(x_1, \dots x_{n-1}))x^{n-k}$, so the conclusion will follow as long as $\epsilon_k(x_1, \dots x_{n-1}) + x_n \epsilon_{k-1}(x_1, \dots x_{n-1}) = \epsilon_k(x_1, \dots x_n)$ which holds because the first summand is the sum of all products of k monomials x_i that don't have x_n as

a factor, while the second one is the sum of all products of k monomials x_i that do have x_n as a factor, while $\epsilon_k(x_1, \dots x_n)$ is just the sum of all products of k monomials x_i.

5. Every monomial ϵ_i of total degree 1 is equivalent to $\epsilon_{(i)}$ under the definition, so if all polynomials of total degree $n-1$ correspond to some ϵ_λ, then any monomial of total degree n is the product of a monomial of total degree $n-1$ and some ϵ_j, so the monomial $\epsilon_{(\lambda,j)}$ is equal to it.

6. $|\lambda_i|$ is the number of nonzero entries in row i of the matrix A representing λ. So $|\lambda_i^*|$ is the number of nonzero entries in row i of A^T, which is the number of nonzero entries in column i of A. $A_{ij} = 1 \leftrightarrow \lambda_i \geq j$, so column j of A has precisely as many nonzero elements as there are entries in λ with size $\geq j$, so $\lambda_j^* = |\{i : \lambda_i \geq j\}|$.

7. $\epsilon_\lambda(x_1, \dots x_n) = \prod_i \epsilon_{\lambda_i}(x_1, \dots x_n)$, and each ϵ_{λ_i} is homogeneous of total degree λ_i, and the product of homogeneous polynomials of degree i and j is a homogeneous polynomial of degree $i+j$, so ϵ_λ is homogeneous of total degree $|\lambda|$.

8. Let $f(x) = \sum_i k_i x^{\alpha_i} \in K_d^S[x_1, \dots x_n]$, where $\alpha_i = (\alpha_{i1}, \alpha_{i2}, \dots \alpha_{in})$ and $\sum_k \alpha_{ik} = d$ for all i, then for each α_i in the expansion f, the orbit of α_i occurs as well in the expansion of f, all with the same coefficient k_i, since f is symmetric. So $f(x) = \sum_i k_i m_{\alpha_i}(x_1, \dots x_n)$. So the m_λ span $K_d^S[x_1, \dots x_n]$, and x^{α_i} and x^{α_j} are linear independent if and only if $\alpha_i \neq \alpha_j$, so the m_λ are linearly independent, so the m_λ are a basis of $K_d^S[x_1, \dots x_n]$.

9. An ϵ_λ of degree d is an integer linear combination of monomials x^α of total degree d by its definition. Since the $m\lambda$ are a basis of $K_d^S[x_1, \dots x_n]$ by the previous exercise, and $\epsilon_\lambda \in K_d^S[x_1, \dots x_n]$, it follows that ϵ_λ is an integer linear combination of m_λ.

10. The determinant of an upper-triangular integer matrix T with ones on the main diagonal is 1 since any permutation of the rows leaves a 0 on the main diagonal, so T has some inverse. The last row of TT^{-1} is the last row of T^{-1} since the last row of T is $(0, 0, \dots 0, 1)$. Therefore, the last row of T^{-1} is also $(0, 0, \dots 0, 1)$, since that is the last row of the identity. The second-to-last row of TT^{-1} is the second-to-last row of T^{-1} plus the last entry in the second-to-last row of T times the last row of T^{-1}. Since the last row of T^{-1} is $(0, 0, \dots 0, 1)$, this implies that the second-to-last-row of T^{-1} is $(0, 0, \dots 1, a)$ where a is arbitrary. So continuing in this way from the last row to the first, it comes about that T^{-1} is upper-triangular with ones on the main diagonal.

11. $m_{331} = x_1^3 x_2^3 x_3 + x_1^3 x_2 x_3^3 + x_1 x_2^3 x_3^3, m_{321} = x_1^3 x_2^2 x_3 + x_1^3 x_2 x_3^2 + x_1^2 x_2^3 x_3 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 + x_1 x_2^2 x_3^3$.

12. Yep.

13. (a) This is $\epsilon_3\epsilon_2$.
    (b) This is example 9.6.9.

14. OK

15. If $x_m = x_n$ for some $m \neq n$, then $f(x_1, \ldots x_n) = 0$ because $\sigma_{mn} f(x_1, \ldots x_n) = -f(x_1, \ldots x_n) = f(x_1, \ldots x_n)$, where σ_{mn} is the permutation interchanging x_m and x_n. So let $h_k(x) = f(x_1, x_2, \ldots x_{k-1}, x, x_{k+1}, \ldots x_n)$, then $h_k(x_m) = 0 \forall m \neq k$, so $(x - x_m)$ divides f for all such m. So $h(x) = \prod_{m \neq k}(x - x_m)g(x)$ where g is arbitrary. So $f(x) = h(x_k) = \prod_{m \neq k}(x_k - x_m)g(x)$. Repeating for all values of $1 \leq k \leq n$, it follows that every $(x_i - x_j)$ where $i \neq j$ divides f. We can conveniently group these values into $f(x) = (\prod_{i<j}(x_i - x_j))g(x)$. Since $\prod_{i<j}(x_i - x_j)$ is antisymmetric and f is antisymmetric, it follows that g is symmetric.

7 The General Equation of Degree n

1. (a) The discriminant is -59, which isn't a square, so the Galois field is S_3.
   (b) The discriminant is 1, which is a square, so the Galois field is A_3.
   (c) The discriminant is -27, which isn't a square, so the Galois field is S_3.

2. $\delta^2(f)$ is negative, so the Galois field is S_3. $\mathbb{Q}(\alpha)$, where α is a root of f, is an extension of degree 3, and $\mathbb{Q}(\delta)$ is an extension of degree 2.

3. The highest lexicographic term in δ^2 is $x_1^{2n-2} x_2^{2n-4} \cdots x_{n-1}^2$, which is the first term of $\epsilon_1^2 \epsilon_2^2 \cdots \epsilon_{n-1}^2$. This is the highest-degree monomial in the expansion of δ^2 in the symmetric polynomials, because any higher-degree monomial in the ϵ would be higher lexicographically. Therefore, δ^2 is a polynomial of degree $2n-2$ in the symmetric polynomials.

4. By the previous exercise, δ^2 is a polynomial in the $\epsilon_k(\alpha_1, \ldots \alpha_n)$, $\delta^2(f) = a_n^{2n-2} \sum_k c_k \epsilon_k^{n_k}$, and by 9.6.4 $\epsilon_k(\alpha_1, \ldots \alpha_n) = (-1)^k a_{n-k}/a_n$, so $\delta^2(f) = a_n^{2n-2} \sum_k c_k((-1)^k a_{n-k}/a_n)^{n_k}$, a symmetric polynomial of degree $2n-2$ in the coefficients a_i.

5. When $n = 2$, $\delta^2(f) = b^2 - 4ac$; when $n = 3$, $\delta^2(f)$ is as in Example 9.7.3.

6. We can compute that f has no root in $\mathbb{Z}_3$, so the only possible factorization is by two irreducible quadratics, but if $f(x) = (ax^2 + bx + c)(a'x^2 + b'x + c') = aa'x^4 + (ab' + a'b)x^3 + (ac' + bb' + a'c)x^2 + (bc' + b'c)x + cc'$, then we must have $aa' = 1, ab' + a'b = 0, ac' + bb' + ca' = 1, bc' + b'c = 1, cc' = 1 \leftrightarrow a = a' \neq 0, c = c' \neq 0 \rightarrow a(b + b') = 0 \rightarrow b + b' = 0$, but also $c(b + b') = 1$, a contradiction that precludes such a factorization, so f is irreducible.

7. Gulp.

8. They are.

9. Let $\{\alpha_i\}$ be the roots of f, $\{\beta_i\}$ be the roots of g, then $f(x) = \prod_i(x-\alpha_i), g(x) = \prod_i(x-\beta_i)$, so $f\psi = g\phi \leftrightarrow \psi(x)\prod_i(x-\alpha_i) = \phi(x)\prod_i(x-\beta_i)$ so each factor $x-\alpha_i$ must divide the right side, and since the degree of ϕ is only at most $n-1$, at least one of the $x-\alpha_i$ must divide $\prod_i(x-\beta_i) = g(x)$, so this $x-\alpha_i$ is a nonconstant common factor of f and g.

10. (a) $R(f,g) = a_n^m b_m^n \prod_i \prod_j (\xi_i - \eta_j) = (-1)^{m+n} a_n^m b_m^n \prod_i \prod_j (\eta_j - \xi_i) = R(g,f)$.
    (b) $g(x) = b_m^n \prod_j (x-\eta_j) \rightarrow a_n^m \prod_i g(\xi_i) = a_n^m b_m^n \prod_i \prod_j (\xi_i - \eta_j) = R(f,g)$.
    (c) Apply b to the right side of a.

11. The product is fixed under permutations of the x_i and the y_j, so it is a polynomial in the symmetric functions on the x_i and on the y_j. Its total degree in the $\epsilon_i(x_1,\dots x_n)$ is m because there's one factor of each x_i for each y_j, a total of m, and similarly the total degree in the $\epsilon_j(y_1,\dots y_n)$ is n.

12. $\det(\mathcal{R}(f,g)) = 0 \leftrightarrow f$ and g have a common root $\leftrightarrow \xi_i = \eta_j$ for some (i,j). Then by the argument of Exercise 9.6.15, $\det(\mathcal{R}(f,g))$ is divisible by $\prod_i \prod_j (\xi_i - \eta_j) = R(f,g)$.

13. Koff

8 Quartic Polynomials

1. $h(y) = (y-\theta_1)(y-\theta_2)(y-\theta_3) = y^3 - (\theta_1+\theta_2+\theta_3)y^2 + (\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3)y - \theta_1\theta_2\theta_3$. And so then $\theta_1+\theta_2+\theta_3 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)+(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)+(\alpha_1+\alpha_4)(\alpha_2+\alpha_3) = 2(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4) = 2\epsilon_2(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = 2p$. And $\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = \epsilon_2(\alpha_1,\alpha_2,\alpha_3,\alpha_4)^2 - 4\epsilon_4$. And $\theta_1\theta_2\theta_3 = \epsilon_3^2$. Thus, by 9.6.4, $h(y) = y^3 - 2py^2 + (p^2-4r)y + q^2$.

2. If α is a root of $f(x)$, then $\alpha - c$ is a root of $f(x+c)$, so $\delta^2(f(x+c)) = \prod_{i<j}(\alpha_i - c - (\alpha_j - c)) = \prod_{i<j}(\alpha_i - \alpha_j) = \delta^2(f)$.

3. Divide the polynomial by the leading coefficient since the roots of $f(x)/a_n$ are the same as the roots of $f(x)$. The roots are all we care about in this section, so that's all you need to do.

4. Consider one factor of the discriminant of h, $(\theta_1-\theta_2)^2 = [(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)-(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)]^2 = [\alpha_1\alpha_3+\alpha_2\alpha_4-\alpha_1\alpha_2-\alpha_3\alpha_4]^2 = [(\alpha_1-\alpha_4)(\alpha_3-\alpha_2)]^2$. Similar computations reveal that the other factors of $\delta^2(h)$ reduce to the other factors of $\delta^2(f)$, $[(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)]^2$ and $[(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)]^2$.

5. If the resolvent polynomial h is not irreducible in K, then at least one of its roots, say θ_1, is in K. The only possibilities are that only $\theta_1 \in K$, or all three of the roots are in K, since a cubic factors into either three linear factors or an irreducible quadratic and a linear factor. If all three of the roots are in K, then $\delta \in K$ and the splitting field of h is $K = K(\delta)$. If only $\theta_1 \in K$, then $\delta \notin K$ by the argument in "case 1B" on page 463, and the splitting field of H is quadratic over K since h factors into a linear factor and an irreducible quadratic. $K(\delta)$ is a subset of the splitting field of h, and it's a nontrivial extension of K since $\delta \notin K$, so since there are no proper intermediate fields between K and any quadratic splitting field it follows that $K(\delta)$ is the splitting field. If h is irreducible, then cases 1A and 1B on page 463 cover all possibilities for the splitting field, and in neither case is it $K(\delta)$.

6. It's irreducible by the Eisenstein Criterion, and the discriminant is 4725, which isn't a square in $\mathbb{Q}$, and the resolvent cubic is $h(x) = x^3 - 12x + 9 = (x-3)(x^2+3x-3)$, which isn't irreducible but doesn't split in $\mathbb{Q}$, so we use the $H(x)$ polynomial from Llama 9.8.1 which is $(x^2+3)(x^2-3x+3)$ which doesn't split, so the Galois field is D_4.

7. It's irreducible by the Eisenstein Criterion, and the discriminant is $256p^3 - 27p^4$, which is 22981 when $p = 7$ and negative for all greater primes, so it's never a square in $\mathbb{Q}$. The resolvent cubic is $h(x) = x^3 - 4px + p^2$, so the only possible linear factors of h are $(x \pm p)$, since the constant term is p^2, so if $x - p$ is a divisor then we get a factorization $h(x) = x^3 + 0x^2 - 4px + p^2 = (x-p)(x^2+bx-p) = x^3 + (b-p)x^2 - (p+b)x + p^2$ for some b, so lining up the quadratic coefficients gives us $b = p$, but lining up the linear coefficients gives us $b = p + 3$, so there is no factorization of h by $x - p$.

   And if $x + p$ is a factor of h then we have a factorization $h(x) = x^3 + 0x^2 - 4px + p^2 = (x+p)(x^2+bx+p) = x^3 + (b+p)x^2 + (p+bp)x + p^2$ for some b, but lining up quadratic coefficients we get $b = -p$, and lining up linear coefficients we get $b + 5 = 0$, so $b = -5$ and $p = 5$ is the only situation where h is factorable, so for $p > 5$, h is irreducible, so the Galois group of $x^4 + px + p$ is S_4.

8. It's irreducible since $x^2 + 5x + 3$ is irreducible, and the discriminant is 8112 which is not a square, and the resolvent cubic is $x^3 - 10x^2 + 13x$, which always has a factor x corresponding to a root $\theta = 0$, so the 9.8.1 polynomial $H(x) = x^2(x^2 - 5x + 3)$, which does not split, so the Galois group is D_4.

9.

10.

11.

9 Galois Groups of Higher Degree Polynomials

1. Erk.