2014 Algebra SEP ~ Standard Field Theory Facts (by Evan Dummit)

- Suggested reading: Dummit/Foote chapter 13 (basic fields), and chapter 14 (Galois theory).
- Basic facts about fields:
  - If E/F is an extension of fields, then the degree $[E:F]$ of the extension is $\dim_F E$, as a vector space.
  - Degree is multiplicative in towers: If $K/E/F$ is a tower, then $[K:F]=[K:E]\cdot[E:F]$. This fact is easy yet extremely useful.
  - If E_1 and E_2 are two extensions of F and E_1E_2 is their composite, then $[E_1E_2:F]\le[E_1:F]\cdot[E_2:F]$, with equality iff a basis for one field over F remains linearly-independent over the other field.
  - For any $\alpha\in E$, the degree of α over F is the extension degree $[F[\alpha]:F]$
    - If this degree of α is finite then α satisfies a unique, monic polynomial (called the minimal polynomial of α) of that degree and is algebraic over F.
    - If the degree of α is infinite then α is transcendental over F.
  - If every element of E is algebraic over F, we say E is an algebraic extension of F. Finite-degree extensions are algebraic: indeed, the degree of the minimal polynomial of any element $\alpha\in E$ over F divides $[E:F]$, since $F[\alpha]$ is a subfield of E.
    - If a field has no algebraic extensions, then we say it is algebraically closed (Example: $\mathbb{C}$.)
    - Every field has an algebraic closure.
    - If E/F is an extension, then the set of elements of E that are algebraic over F is a subfield of E.
  - The field K is a splitting field for $p(x)\in F[x]$ if $p(x)$ factors completely into a product of linear factors over K but does not factor completely over any subfield of K (containing F). An extension K/F which is the splitting field over F for a collection of some polynomials is called a normal extension.
    - If $p(x)\in F[x]$ is any polynomial then (up to isomorphism) it has a unique splitting field over F.
  - A polynomial $q(x)\in F[x]$ is separable if it has no multiple roots; otherwise it is inseparable.
    - Irreducible inseparable polynomials can only exist in characteristic p, and such a polynomial can be written uniquely in the form $q(x)=q_{\text{sep}}(x^{p^k})$ where $q_{\text{sep}}(x)$ is separable and k is a positive integer.
    - A field extension is separable if the minimal polynomial of every element is separable; an extension is inseparable otherwise.
- Basic facts about Galois theory:
  - If E/F is an extension of fields, then $\text{Aut}(E/F)$ is the group of automorphisms of E fixing F.
  - If E is the splitting field of $f(x)$ over F, then $|\text{Aut}(E/F)|\le[E:F]$ with equality if and only if f is separable over F. In such a case, the extension E/F is Galois, and $\text{Aut}(E/F)$ is called the Galois group.
    - In other words, an extension is Galois iff it is normal and separable.
  - (Fundamental Theorem of Galois Theory) If K/F is a Galois extension and $G=\text{Gal}(K/F)$, then there is a bijection between subfields E of K containing F and subgroups of G, given by the correspondences $E\to\{\text{elements of } G \text{ fixing } E\}$ and $\{\text{the fixed field of } H\}\leftarrow H$.
    - If E is a subfield corresponding to a subgroup H, then $[K:E]=|H|$ and $[E:F]=|G:H|$.
    - Normal subgroups in the subgroup lattice correspond to Galois extensions in the subfield lattice. In particular, K/E is always Galois.
    - If E_1,E_2 correspond to H_1,H_2, then the composite E_1E_2 corresponds to $H_1\cap H_2$ and $E_1\cap E_2$ corresponds to $\langle H_1,H_2\rangle$.
    - In summary: the subgroup lattice of G is the same as the upside-down subfield lattice of K.
    - ("Sliding-up" property) If K/F is Galois and F'/F is any extension, then KF'/F' is Galois and $\text{Gal}(KF'/F')\cong\text{Gal}(K/K\cap F')$. In particular, $[KF':F]\cdot[K\cap F':F]=[K:F]\cdot[F':F]$.
    - If K_1 and K_2 are Galois over F, then $K_1\cap K_2$ and K_1K_2 are Galois over F, and $\text{Gal}(K_1K_2/F)$ is isomorphic to the subgroup of $\text{Gal}(K_1/F)\times\text{Gal}(K_2/F)$ of elements whose restrictions to $K_1\cap K_2$ are equal.

- (Primitive Element Theorem) If K/F is a finite-degree, separable extension, then $K = F[\alpha]$ for some $\alpha \in K$.
- If $p(x) \in F[x]$ is a polynomial of degree n, its Galois group is the Galois group of its splitting field K over F.
  - Any element of $G = \mathrm{Gal}(K/F)$ permutes the roots of $p(x)$ and, conversely, is determined by its action on the roots of p, so if we choose an ordering of the roots we obtain an embedding of $\mathrm{Gal}(K/F)$ into S_n. In general, one freely thinks of the Galois group as a subgroup of S_n.
  - G is a transitive subgroup of S_n (i.e., there exists an element of G taking any root of p to any other root of p) if and only if $p(x)$ is irreducible.
  - If $\mathrm{char}(F) \neq 2$, G is a subgroup of A_n if and only if the square root of the discriminant $\sqrt{D} = \prod_{i<j}(x_i - x_j)$ of $p(x)$ lies in F, where the x_i are the roots of p.

- Basic facts about cyclotomic and radical extensions:
  - If ζ is a root of unity (that is, $\zeta^n = 1$), then $K[\zeta]$ is called a cyclotomic extension of K.
  - If ζ_n is a primitive nth root of unity, then $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$ with abelian Galois group of order $\varphi(n)$, isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, where the isomorphism is given explicitly by $a \mapsto [\zeta_n \mapsto \zeta_n^a]$. In particular, cyclotomic extensions of $\mathbb{Q}$ are abelian.
    - By using a special case of Dirichlet's theorem on primes in arithmetic progression (that says there exists a prime that is 1 mod n for any n), one can use the above to show that every abelian group occurs as a Galois group over $\mathbb{Q}$.
  - (Kronecker-Weber) Every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension.
  - If F has characteristic not dividing n, $a \in F$, and F contains the nth roots of unity, then $F(a^{1/n})$ is a cyclic extension of F of degree dividing n. An extension of this type is called a (simple) radical extension. Conversely, with the same assumptions on F, every cyclic extension of F is of that form $F(a^{1/n})$.
  - A polynomial can be solved by radicals if all its roots lie in some tower of simple radical extensions.
  - (Solvability by Radicals) The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.

- Basic facts about finite fields:
  - If $\mathbb{F}_{q^n}/\mathbb{F}_q$ is any extension of finite fields, then the Galois group is cyclic and generated by the qth-power Frobenius map $x \mapsto x^q$. Every other basic property of finite fields can be deduced from this fact: there is a unique finite field (up to isomorphism) of any prime-power order, $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n} - x$, the intermediate extensions between $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ are $\mathbb{F}_{q^d}$ where $d|n$, and so forth.

- Useful tricks:
  - If f is an irreducible polynomial with α and $g(\alpha)$ as roots, then g is (morally) an element of the Galois group of f, and it is useful to think of it as such.
  - If K/F is a Galois extension and $\alpha \in K$ is fixed by all elements of the Galois group $\mathrm{Gal}(K/F)$, then $\alpha \in F$. This fact, while obvious from the Galois correspondence, is often very useful.
  - If $m(x) \in F[x]$ is the minimal polynomial over F of some α, then if $f(x) \in F[x]$ is any other polynomial with $f(\alpha) = 0$, then $m(x)$ divides $f(x)$. [Reason: minimal polynomials are irreducible. Then $\gcd(m, f)$ divides $m(x)$ and has positive degree, hence it must be m. This argument shows up a lot.]
  - In analyzing relatively simple field extensions, one often needs to calculate degrees of field extensions. Frequently Eisenstein's criterion is useful for this:
    - If $f(x) \in R[x]$ is a monic polynomial over a UFD, and all coefficients of $f(x)$ lie in a prime ideal P but the constant term of $f(x)$ does not lie in P^2, then $f(x)$ is irreducible.
  - If you are in characteristic zero and you have a non-Galois field extension, it is usually a good idea to try looking at the Galois closure of the extension, and analyze how the Galois group of this extension acts on the original extension.
  - If you are in positive characteristic, be very careful about inseparable extensions. If the problem involves pth powers in characteristic p, you may have to worry that the extension is inseparable (to check whether a polynomial f is inseparable, see if f and f' have any common roots). If you do have an inseparable polynomial, your best bet is to try to resort to explicit calculations whenever possible.