Modern Algebra II Spring 2019
Review Sheet for the Final

Let R be a UFD and let K be its field of quotients. An element $r/s \in K$ is in *lowest terms* if r and s are relatively prime, and every element of K can be written in this way. We recall:

Lemma: Let R be a UFD and let $r \in R$, $r \neq 0$. Then r is irreducible $\iff$ the ideal (r) is a prime ideal.

Let R be an integral domain (not necessarily a UFD). If I is an ideal of R, then we have the natural homomorphism $\pi\colon R \to R/I$ as well as $R[x] \to (R/I)[x]$, also denoted by π, which we sometimes call *reduction mod* I. We sometimes denote $\pi(f)$ by $\bar{f}$. Note that $\deg \bar{f} \leq \deg f$, with equality $\iff$ the leading coefficient of f is not in I.

Rational roots test: Let R be a UFD with field of quotients K and let $f = a_n x^n + \cdots + a_0 \in R[x]$. Suppose that $p/q \in K$ with $p, q \in R$, $\gcd(p, q) = 1$, and p/q is a root of f. Then $p | a_0$ and $q | a_n$.

Theorem: Let R be a UFD with field of quotients K and let $f = a_n x^n + \cdots + a_0 \in R[x]$ have degree $n \geq 1$. Then there exist polynomials $g_1, h_1 \in K[x]$ with $\deg g_1 = d < \deg f$ and $\deg h_1 = e < \deg f$ such that $f = g_1 h_1$ if and only if there exist polynomials $g, h \in R[x]$ with $\deg g = d$ and $\deg h = e$ such that $f = gh$.

Corollary: Let R be a UFD with field of quotients K and let $f \in R[x]$ have degree $n \geq 1$. If f does not factor into a product of polynomials in $R[x]$ of strictly smaller degrees, then f is irreducible in $K[x]$.

Lemma (holds for every integral domain R, not necessarily a UFD): Let R be an integral domain and let I be an ideal of R. Denote by $\bar{f}$ the image of f in $(R/I)[x]$. If $f \in R[x]$ and the leading coefficient of f is not in I, and if $f = gh$, then $\deg \bar{g} = \deg g$ and $\deg \bar{h} = \deg h$.

Theorem: Let R be a UFD with field of quotients K and let I be an ideal of R. Let $f = a_n x^n + \cdots + a_0 \in R[x]$ have degree $n \geq 1$ and suppose that $\bar{f} = \bar{a}_n x^n + \cdots + \bar{a}_0 \in (R/I)[x]$ is the reduction of f mod I. If $a_n \notin I$ and $\bar{f}$ does not factor into a product of polynomials in $(R/I)[x]$ of strictly smaller degrees, then f does not factor into a product of polynomials in $R[x]$ of strictly smaller degrees, and hence f is irreducible in $K[x]$.

Theorem (Eisenstein criterion): Let R be a UFD with field of quotients K and let M be a maximal ideal of R. Let $f = a_n x^n + \cdots + a_0 \in R[x]$ have degree $n \geq 1$. Suppose that

1. $a_n \notin M$;

2. For all $i < n$, $a_i \in M$;

3. $a_0 \notin M^2$.

Then f does not factor into a product of polynomials in $R[x]$ of strictly smaller degrees, and hence f is irreducible in $K[x]$.

Proposition: Let p be a prime number and let $\Phi_p \in \mathbb{Q}[x]$ be the pth *cyclotomic polynomial*:

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Then Φ_p is irreducible in $\mathbb{Q}[x]$.

If $f = a_n x^n + \cdots + a_0 \in R[x]$ with $f \neq 0$, we define the *content* $c(f)$ to be the gcd of the coefficients $a_n, \ldots, a_0$. It is well defined up to a unit. A nonzero polynomial $f \in R[x]$ is *primitive* if $c(f) = 1$. Every nonzero polynomial $f \in R[x]$ can be written as $f = c(f) f_0$, where f_0 is primitive.

Lemmas used for proving the theorem stated after the rational roots test on the previous page:

Lemma 1: Let R be a UFD with field of quotients K. Suppose that $f, g \in R[x]$ are both primitive and that there exists an $\alpha \in K^*$ with $\alpha f = g$. Then $\alpha \in R$ and α is a unit.

Lemma 2: Let R be a UFD with field of quotients K. Suppose that $f \in K[x]$ with $\deg f \geq 1$. Then there exists $\alpha \in K^*$ such that $\alpha f \in R[x]$ and αf is primitive.

Lemma 3 (Gauss lemma): Let R be a UFD with field of quotients K. Suppose that $f, g \in R[x]$ are both primitive. Then fg is primitive.

As a corollary of the theorem stated earlier, we also have:

Proposition: Let R be a UFD with field of quotients K and let $f \in R[x]$ be a polynomial of degree at least one. Then f is irreducible in $R[x] \iff$ f is primitive and f is irreducible in $K[x]$.

These results can also be used to prove:

Theorem: Let R be a UFD with field of quotients K. Then $R[x]$ is also a UFD. Moreover, the irreducibles in $R[x]$ are either

1. irreducibles $r \in R$, viewed as polynomials of degree 0, or

2. primitive polynomials $f \in R[x]$ such that f is irreducible in $K[x]$.

Corollary: The following rings are UFD's: $F[x_1, \ldots, x_n]$, where F is a field; $\mathbb{Z}[x_1, \ldots, x_n]$; $R[x_1, \ldots, x_n]$ where R is a UFD.

Throughout the rest of this review sheet, F denotes a **field** and E is an extension field of F.

Definition: Let E be a finite extension of a field F. Then the *Galois group* $\mathrm{Gal}(E/F)$ is the set of automorphisms $\sigma\colon E \to E$ such that $\sigma(a) = a$ for all $a \in F$. It is a group under function composition. If H is a subgroup of $\mathrm{Gal}(E/F)$, then the *fixed field* E^H is

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

It is a subfield of E containing F.

Clearly, if $F \leq K \leq E$, then $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$ and, if $H_1 \leq H_2 \leq \mathrm{Gal}(E/F)$, then $E^{H_2} \leq E^{H_1}$. In other words, both constructions are *order reversing*.

Proposition: Suppose that E is a finite extension of F. Let $f \in F[x]$, let $\alpha \in E$, and let $\sigma \in \mathrm{Gal}(E/F)$. Then α is a root of $f \iff \sigma(\alpha)$ is a root of f.

More generally, suppose that E is a finite extension of F. Let $\sigma\colon F \to K$ be a homomorphism, where K is also a field, let L be an extension field of K, and let $\varphi\colon E \to L$ be a homomorphism such that $\varphi(a) = \sigma(a)$ for all $a \in F$. In this case, we call φ an *extension* of σ. Then, given $f \in F[x]$ and $\alpha \in E$

$$\varphi(f(\alpha)) = (\sigma(f))(\varphi(\alpha)).$$

Hence α is a root of $f \iff \varphi(\alpha)$ is a root of $\sigma(f) \in K[x]$.

Proposition: Let E be a finite extension of F, let $f \in F[x]$, and let $\alpha_1, \ldots, \alpha_k \in E$ be the set of all of the roots of f in E. Then for every $\sigma \in \mathrm{Gal}(E/F)$, σ permutes the set $\{\alpha_1, \ldots, \alpha_k\}$. The function $(\sigma, \alpha_i) \mapsto \sigma(\alpha_i)$ defines an action of $\mathrm{Gal}(E/F)$ on the set $\{\alpha_1, \ldots, \alpha_k\}$ and hence a homomorphism $\rho\colon \mathrm{Gal}(E/F) \to S_k$ (where S_k is the group of permutations of $\{1, \ldots, k\}$ or equivalently of $\{\alpha_1, \ldots, \alpha_k\}$). Finally, if $E = F(\alpha_1, \ldots, \alpha_k)$, then ρ is injective and thus identifies the group $\mathrm{Gal}(E/F)$ with a subgroup of the symmetric group S_k.

Corollary: If E is a finite extension of F, then the group $\mathrm{Gal}(E/F)$ is finite.

Lemma: Let F be a field, let $E = F(\alpha)$ be a simple extension of F, where α is algebraic over F and $f = \mathrm{irr}(\alpha, F)$, let $\sigma\colon F \to K$ be a homomorphism from F to a field K, and let L be an extension of K. If $\beta \in L$ is a root of

$\sigma(f)$, then there is a unique extension of σ to a homomorphism $\varphi\colon E \to L$ such that $\varphi(\alpha) = \beta$.

Hence there is a bijection from the set of homomorphisms $\varphi\colon E \to L$ such that $\varphi(a) = \sigma(a)$ for all $a \in F$ to the set of roots of the polynomial $\sigma(f)$ in L, where $\sigma(f) \in K[x]$ is the polynomial obtained by applying the homomorphism σ to coefficients of f.

Theorem (Isomorphism Extension Theorem): Let E be a finite extension of a field F. Let K be a field and let $\sigma\colon F \to K$ be a homomorphism. Then:

(i) There exist at most $[E : F]$ homomorphisms $\varphi\colon E \to K$ extending σ, i.e. such that $\varphi(\alpha) = \sigma(\alpha)$ for all $\alpha \in F$.

(ii) There exists an extension field L of K and a homomorphism $\varphi\colon E \to L$ extending σ.

(iii) If F has characteristic zero (or F is finite or more generally perfect), then there exists an extension field L of K such that there are exactly $[E : F]$ homomorphisms $\varphi\colon E \to L$ extending σ.

Corollary: Let E be a finite extension of F. Then

$$\#(\mathrm{Gal}(E/F)) \leq [E : F].$$

Definition. Let E be a finite extension of F. Then E is a *separable* extension of F if, for every extension field K of F, there exists an extension field L of K such that there are exactly $[E : F]$ homomorphisms $\varphi\colon E \to L$ with $\varphi(a) = a$ for all $a \in F$.

Theorem: A finite extension E of a field F is a separable extension $\iff$ for all $\alpha \in E$, the polynomial $\mathrm{irr}(\alpha, F, x)$ does not have multiple roots.

For example, if F has characteristic zero or is finite or more generally is perfect, then every finite extension of F is separable.

Theorem (Primitive Element Theorem): Let E be a finite separable extension of the field F. Then E is a simple extension of F, i.e. there exists an $\alpha \in E$ such that $E = F(\alpha)$.

Definition: Let F be a field and let $f \in F[x]$ be a polynomial of degree at least 1. Then an extension field E of F is a *splitting field* for f over F if the following two conditions hold:

(i) In $E[x]$, there is a factorization $f = c\prod_{i=1}^{n}(x - \alpha_i)$. In other words, f factors in $E[x]$ into a product of linear factors.

(ii) With the notation of (i), $E = F(\alpha_1, \ldots, \alpha_n)$. In other words, E is generated as an extension field of F by the roots of f.

Note: one can show that, if E_1 and E_2 are two splitting fields for f over F, then there exists an isomorphism $\varphi\colon E_1 \to E_2$ such that $\varphi(a) = a$ for all $a \in F$. Thus we can (and often do) speak of **the** splitting field for f over F.

Theorem: Let E be a finite extension of a field F. Then the following are equivalent:

(i) There exists a polynomial $f \in F[x]$ of degree at least one such that E is a splitting field of f.

(ii) For every extension field L of E, if $\varphi\colon E \to L$ is a homomorphism such that $\varphi(a) = a$ for all $a \in F$, then $\varphi(E) = E$, and hence φ is an automorphism of E, in fact $\varphi \in \mathrm{Gal}(E/F)$.

(iii) For every **irreducible** polynomial $p \in F[x]$, if there is a root of p in E, then p factors into a product of linear factors in $E[x]$.

Definition: Let E be a finite extension of F. If any one of the equivalent conditions of the preceding theorem is fulfilled, we say that E is a *normal* extension of F.

Corollary: Let E be a finite extension of a field F. Then the following are equivalent:

(i) E is a separable extension of F (this is automatic if the characteristic of F is 0 or F is finite or perfect) and E is a normal extension of F.

(ii) $\#(\mathrm{Gal}(E/F)) = [E : F]$.

Definition: A finite extension E of a field F is a *Galois extension* of F if and only if $\#(\mathrm{Gal}(E/F)) = [E : F]$. Thus, the preceding corollary can be rephrased as saying that E is a Galois extension of F if and only if E is a normal and separable extension of F.

Important remark: There exist sequences of extensions $F \leq K \leq E$ where K is a normal extension of F and E is a normal extension of K, but E is **not** a normal extension of F. Likewise, there exist sequences of extensions $F \leq K \leq E$ where E is a normal extension of F, but K is **not** a normal extension of F. **Note:** It is automatic that, if $F \leq K \leq E$ and E is a normal extension of F, then E is a normal extension of K.

Theorem (Main Theorem of Galois Theory): Let E be a **Galois** extension of a field F. Then:

(i) There is a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields K between F and E, given as follows: To a subgroup H of $\mathrm{Gal}(E/F)$, we associate the fixed field E^H, and to an intermediate field K between F and E we associate the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$. These constructions are inverses, in other words

$$\begin{aligned} \mathrm{Gal}(E/E^H) &= H; \\ E^{\mathrm{Gal}(E/K)} &= K. \end{aligned}$$

In particular, the fixed field of the full Galois group $\mathrm{Gal}(E/F)$ is F and the fixed field of the identity subgroup is E: $E^{\mathrm{Gal}(E/F)} = F$ and $E^{\{1\}} = E$. Finally, since there are only finitely many subgroups of $\mathrm{Gal}(E/F)$, there are only finitely many intermediate fields K between F and E.

(ii) The above correspondence is order reversing with respect to inclusion.

(iii) For every subgroup H of $\mathrm{Gal}(E/F)$, $[E : E^H] = \#(H)$, and hence

$$[E^H : F] = (\mathrm{Gal}(E/F) : H) = \#(\mathrm{Gal}(E/F))/\#(H).$$

Likewise, for every intermediate field K between F and E,

$$\#(\mathrm{Gal}(E/K)) = [E : K],$$

and hence

$$(\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)) = \#(\mathrm{Gal}(E/F))/\#(\mathrm{Gal}(E/K)) = [K : F].$$

(iv) For every intermediate field K between F and E, the field K is a **normal** extension of F if and only if $\mathrm{Gal}(E/K)$ is a **normal** subgroup of $\mathrm{Gal}(E/F)$. In this case, K is a Galois extension of F, and

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \Big/ \mathrm{Gal}(E/K).$$

Let F be a field, which for simplicity we assume from now on **to be of characteristic** 0, and let $f \in F[x]$ be a nonzero polynomial. We define the *Galois group of* f (over F, if this is not clear from the context) to be the Galois group $\mathrm{Gal}(E/F)$, where E is a splitting field for f over F.

Proposition: Suppose that f is an irreducible polynomial in $F[x]$ of degree $n \geq 1$. Then n divides the order of the Galois group of f and the order of the Galois group of f divides $n!$.

Definition: A Galois extension E of F is *abelian* if $\mathrm{Gal}(E/F)$ is an abelian group. In this case, every subgroup of $\mathrm{Gal}(E/F)$ is a normal subgroup, hence every intermediate subfield K (i.e. $F \leq K \leq E$) is a normal extension of F.

Cyclotomic extensions: Let E be an extension field of F and suppose that E is a splitting field of $x^n - 1$, i.e. that, if $\mu_n(E) \subseteq E$ is the set of roots of $x^n - 1$ in E, then $\#(\mu_n(E)) = n$. Since $\mu_n(E)$ is cyclic, there exists a $\zeta \in \mu_n(E)$ which is a generator of $\mu_n(E)$, i.e. $\mu_n(E) = \langle \zeta \rangle$, and hence $E = F(\zeta)$. For every $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\zeta) = \zeta^i$ for some i relatively prime to n. The function $\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^*$ which associates to an element $\sigma \in \mathrm{Gal}(E/F)$ the unique $i \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\sigma(\zeta) = \zeta^i$ is an injective homomorphism. Thus $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and hence is abelian.

n^{th} root extensions: suppose that $\mu_n(F) \subseteq F$ satisfies $\#(\mu_n(F)) = n$, i.e. that $x^n - 1$ splits into linear factors in $F[x]$. Let $a \in F$ and let E be a splitting field of $x^n - a$. If $\alpha = \sqrt[n]{a}$ is some root of $x^n - 1$ in E, then every root of $x^n - a$ is of the form $\zeta\alpha$, $\zeta \in \mu_n(F)$. Hence $x^n - a = \prod_{\zeta \in \mu_n}(x - \zeta\alpha)$ and $E = F(\alpha) = F(\sqrt[n]{a})$. For every $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\alpha) = \zeta\alpha$ for a unique $\zeta \in \mu_n(F)$, and this defines an injective homorphism from the Galois group $\mathrm{Gal}(E/F)$ to a subgroup of $\mu_n(F) \cong \mathbb{Z}/n\mathbb{Z}$. Thus $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of a cyclic group and hence is also cyclic, of order dividing n. In particular, (under the assumption that $\#(\mu_n(F)) = n$) E is an abelian extension of F.

The discriminant: Let $f \in F[x]$ have degree $n \geq 1$ and let E be a splitting field for f over F, so that the Galois group of f over F is $\mathrm{Gal}(E/F)$. Suppose that the roots of f in E are $\alpha_1, \ldots, \alpha_n$, so that $\mathrm{Gal}(E/F)$ is identified with a subgroup of S_n. We want to describe when the image of $\mathrm{Gal}(E/F)$ is actually contained in the subgroup A_n of S_n (here A_n is the alternating group). To do so, define the *discriminant of* f by:

$$\Delta = \Delta(f) = \left(\prod_{i<j} (\alpha_j - \alpha_i) \right)^2 .$$

Then there is a given square root $\sqrt{\Delta}$ of Δ defined by $\sqrt{\Delta} = \prod_{i<j}(\alpha_j - \alpha_i)$, and $\sqrt{\Delta} \in E$. From one of the definitions of the sign of a permutation, it is

easy to see that, identifying an element $\sigma \in \mathrm{Gal}(E/F)$ with the corresponding permutation of $\{\alpha_1, \ldots, \alpha_n\}$, or equivalently of $\{1, \ldots, n\}$, then

$$\sigma(\sqrt{\Delta}) = \pm\sqrt{\Delta} = \mathrm{sign}(\sigma)\sqrt{\Delta},$$

where $\mathrm{sign}(\sigma)$ (sometimes written $\varepsilon(\sigma)$) is the unique homomorphism $S_n \to \{\pm 1\}$ whose kernel is A_n. Then $\sigma(\Delta) = \sigma((\sqrt{\Delta})^2) = (\pm\sqrt{\Delta})^2 = \Delta$ for all $\sigma \in \mathrm{Gal}(E/F)$, hence $\Delta \in E^{\mathrm{Gal}(E/F)} = F$. Moreover, $\sigma \in A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$. Hence we see:

Proposition: Suppose that $\Delta \neq 0$. With notation as above, let $\sigma \in \mathrm{Gal}(E/F)$. Then $\sigma \in A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$. Hence $\mathrm{Gal}(E/F)$ is contained in $A_n \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\sqrt{\Delta}) = \sqrt{\Delta} \iff \sqrt{\Delta} \in E^{\mathrm{Gal}(E/F)} = F \iff \Delta$ is a square in F.