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 $\pi: R \to R/I$ as well as $R[x] \to (R/I)[x]$, also denoted by $\pi$, which we sometimes call reduction mod $I$. We sometimes denote $\pi(f(x))$ by $\bar{f}(x)$. Note that $\deg \bar{f}(x) \leq \deg f(x)$, with equality $\iff$ the leading coefficient of $f(x)$ is not in $I$.

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

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

Corollary: Let $R$ be a UFD with field of quotients $K$ and let $f(x) \in R[x]$ have degree $n \geq 1$. If $f(x)$ does not factor into a product of polynomials in $R[x]$ of strictly smaller degrees, then $f(x)$ 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 $\bar{f}(x)$ the image of $f(x)$ in $R/I$.[x]. If $f(x) \in R[x]$ and the leading coefficient of $f(x)$ is not in $I$, and if $f(x) = g(x)h(x)$, then $\deg \bar{g}(x) = \deg g(x)$ and $\deg \bar{h}(x) = \deg h(x)$.

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

Proposition: Let \( p \) be a prime number and let \( \Phi_p(x) \in \mathbb{Q}[x] \) be the \( p \)th cyclotomic polynomial:

\[
\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.
\]

Then \( \Phi_p(x) \) is irreducible in \( \mathbb{Q}[x] \).

If \( f(x) = a_n x^n + \cdots + a_0 \in R[x] \) with \( f(x) \not= 0 \), 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 \( f(x) \in R[x] \) is primitive if \( c(f) = 1 \). Every nonzero polynomial \( f(x) \in R[x] \) can be written as \( f(x) = c(f)f_0(x) \), where \( f_0(x) \) 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 \( f(x), g(x) \in R[x] \) are both primitive and that there exists an \( \alpha \in K^* \) with \( \alpha f(x) = g(x) \). Then \( \alpha \in R \) and \( \alpha \) is a unit.

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

Lemma 3 (Gauss lemma): Let \( R \) be a UFD with field of quotients \( K \). Suppose that \( f(x), g(x) \in R[x] \) are both primitive. Then \( f(x)g(x) \) 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 \( f(x) \in R[x] \) be a polynomial of degree at least one. Then \( f(x) \) is irreducible in \( R[x] \) if and only if \( f(x) \) is primitive and \( f(x) \) 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 \( f(x) \in R[x] \) such that \( f(x) \) 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 \( \text{Gal}(E/F) \) is the set of automorphisms \( \sigma: E \to E \) such that \( \sigma(a) = a \) for all \( a \in F \). It is a group under function composition. If \( H \) is a subgroup of \( \text{Gal}(E/F) \), 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 \( \text{Gal}(E/K) \leq \text{Gal}(E/F) \) and, if \( H_1 \leq H_2 \leq \text{Gal}(E/F) \), 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 \( f(x) \in F[x] \), let \( \alpha \in E \), and let \( \sigma \in \text{Gal}(E/F) \). Then \( \alpha \) is a root of \( f(x) \iff \sigma(\alpha) \) is a root of \( f(x) \).

More generally, suppose that \( E \) is a finite extension of \( F \), \( f(x) \in F[x] \), and \( \alpha \in E \). Let \( \psi: E \to K \) be a homomorphism, where \( K \) is also a field, and let \( \psi(F) = F' \) be the corresponding subfield of \( K \). Then \( \alpha \) is a root of \( f(x) \iff \psi(\alpha) \) is a root of \( \psi(f)(x) \in F'[x] \).

Proposition: Let \( E \) be a finite extension of \( F \), let \( f(x) \in F[x] \), and let \( \alpha_1, \ldots, \alpha_k \in E \) be the set of all of the roots of \( f(x) \) in \( E \). Then for every \( \sigma \in \text{Gal}(E/F) \), \( \sigma \) permutes the set \( \{\alpha_1, \ldots, \alpha_k\} \). The function \( (\sigma, \alpha_i) \mapsto \sigma(\alpha_i) \) defines an action of \( \text{Gal}(E/F) \) on the set \( \{\alpha_1, \ldots, \alpha_k\} \) and hence a homomorphism \( \rho: \text{Gal}(E/F) \to S_k \) (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 \( \rho \) is injective and thus identifies the group \( \text{Gal}(E/F) \) with a subgroup of the symmetric group \( S_k \).

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

Lemma: Let \( F \) be a field, let \( E = F(\alpha) \) be a simple extension of \( F \), where \( \alpha \) is algebraic over \( F \), and let \( K \) be an extension field of \( E \). Let \( f(x) = \text{irr}(\alpha, F, x) \). Then there is a one-to-one correspondence between homomorphisms \( \sigma: E \to K \) such that \( \sigma(a) = a \) for all \( a \in F \) and roots of the
polynomial $f(x)$ in $K$, defined by sending $\sigma$ to $\sigma(\alpha)$ (which thus is a root of $f(x)$).

A slight generalization of the proof of the above lemma shows:

Lemma: Let $F$ be a field, let $E = F(\alpha)$ be a simple extension of $F$, where $\alpha$ is algebraic over $F$, and let $\psi: F \to K$ be a homomorphism from $F$ to a field $K$. Let $f(x) = \text{irr}(\alpha, F, x)$. Then there is a one-to-one correspondence between homomorphisms $\sigma: E \to K$ such that $\sigma(a) = \psi(a)$ for all $a \in F$ and roots of the polynomial $\psi(f)(x)$ in $K$, where $\psi(f)(x) \in K[x]$ is the polynomial obtained by applying the homomorphism $\psi$ to the coefficients of $f(x)$.

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

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

(ii) There exists an extension field $L$ of $K$ and a homomorphism $\sigma: E \to L$ extending $\psi$.

(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 $\sigma: E \to L$ extending $\psi$.

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

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

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

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 $f(x) \in F[x]$ be a polynomial of degree at least 1. Then an extension field $E$ of $F$ is a splitting field for $f(x)$ over $F$ if the following two conditions hold:
(i) In $E[x]$, there is a factorization $f(x) = c \prod_{i=1}^{n}(x - \alpha_i)$. In other words, $f(x)$ 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 $f(x)$.

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

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

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

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

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


Definition: A finite extension $E$ of a field $F$ is a Galois extension of $F$ if and only if $\#(\text{Gal}(E/F)) = [E : F]$. 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 \( \text{Gal}(E/F) \) and intermediate fields \( K \) between \( F \) and \( E \), given as follows: To a subgroup \( H \) of \( \text{Gal}(E/F) \), we associate the fixed field \( E^H \), and to an intermediate field \( K \) between \( F \) and \( E \) we associate the subgroup \( \text{Gal}(E/K) \) of \( \text{Gal}(E/F) \). These constructions are inverses, in other words

\[
\text{Gal}(E/E^H) = H; \\
E^{\text{Gal}(E/K)} = K.
\]

In particular, the fixed field of the full Galois group \( \text{Gal}(E/F) \) is \( F \) and the fixed field of the identity subgroup is \( E \): \( E^{\text{Gal}(E/F)} = F \) and \( E^{(1)} = E \). Finally, since there are only finitely many subgroups of \( \text{Gal}(E/F) \), 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 \( \text{Gal}(E/F) \), \( [E : E^H] = \#(H) \), and hence \( [E^H : F] = (\text{Gal}(E/F) : H) \). Likewise, for every intermediate field \( K \) between \( F \) and \( E \), \( \#(\text{Gal}(E/K)) = [E : K] \) and hence

\[
(\text{Gal}(E/F) : \text{Gal}(E/K)) = [K : F].
\]

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

\[
\text{Gal}(K/F) \cong \text{Gal}(E/F) / \text{Gal}(E/K).
\]

Let \( F \) be a field, which for simplicity we assume from now on to be of characteristic 0, and let \( f(x) \in F[x] \) be a nonzero polynomial. We define the Galois group of \( f(x) \) (over \( F \), if this is not clear from the context) to be the Galois group \( \text{Gal}(E/F) \), where \( E \) is a splitting field for \( f(x) \) over \( F \).
Proposition: Suppose that \( f(x) \) is an irreducible polynomial in \( F[x] \) of degree \( n \geq 1 \). Then \( n \) divides the order of the Galois group of \( f(x) \) and the order of the Galois group of \( f(x) \) divides \( n! \).

Definition: A Galois extension \( E \) of \( F \) is abelian if \( \text{Gal}(E/F) \) is an abelian group. In this case, every subgroup of \( \text{Gal}(E/F) \) 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 \( \mu_n \subseteq E \). Since \( \mu_n \) is cyclic, there exists a \( \zeta_0 \in \mu_n \) which is a generator of \( \mu_n \), i.e. \( \mu_n = \langle \zeta_0 \rangle \), and hence \( E = F(\zeta_0) \). For every \( \sigma \in \text{Gal}(E/F) \), \( \sigma(\zeta_0) = \zeta_0^i \) for some \( i \) relatively prime to \( n \). Thus \( \text{Gal}(E/F) \) is isomorphic to a subgroup of \((\mathbb{Z}/n\mathbb{Z})^*\) and hence is abelian.

\( n \)th root extensions: suppose that \( \mu_n \subseteq F \), 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 \( \zeta \alpha \), \( \zeta \in \mu_n \subseteq F \). Hence \( x^n - a = \prod_{\zeta \in \mu_n}(x - \zeta \sqrt[n]{a}) \) and \( E = F(\sqrt[n]{a}) \). For every \( \sigma \in \text{Gal}(E/F) \), \( \sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a} \) for a unique \( \zeta \in \mu_n \), and this defines an isomorphism from the Galois group \( \text{Gal}(E/F) \) to a subgroup of \( \mu_n \cong \mathbb{Z}/n\mathbb{Z} \). Thus (under the assumption that \( \mu_n \subseteq F \)) \( E \) is an abelian extension of \( F \).

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

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

Then there is a given square root \( \sqrt{\Delta} \) of \( \Delta \) 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 \( \sigma \in \text{Gal}(E/F) \) with the corresponding permutation of \( \{\alpha_1, \ldots, \alpha_n\} \), or equivalently of \( \{1, \ldots, n\} \), then

\[
\sigma(\sqrt{\Delta}) = \pm \sqrt{\Delta} = \text{sign}(\sigma) \sqrt{\Delta},
\]

where \( \text{sign}(\sigma) \) (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 \( \sigma \in \text{Gal}(E/F) \), hence \( \Delta \in E^{\text{Gal}(E/F)} = F \). Moreover, \( \sigma \in A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta} \). Hence we see:

Proposition, with notation as above, \( \text{Gal}(E/F) \) is contained in \( A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta} \) for all \( \sigma \in \text{Gal}(E/F) \iff \sqrt{\Delta} \in E^{\text{Gal}(E/F)} = F \iff \Delta \) is a square in \( F \).