

Derrick Stolee – Math 818 – Midterm Study Guide

For Exam 1:

Def: Ring, Commie Ring, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, Gaussian Integers, $\mathcal{C}[0, 1]$, Field, units: R^\times , Division Ring.

Polynomial Ring: $R[x] = \{\sum_{i=0}^{\infty} r_i x^i \mid r_i \in R, r_i = 0 \text{ for all but finite number of } i.\}$

Def: Subring, Ring Homomorphism, Isomorphism, Endomorphism, Automorphism.

“Substitution Principle” Given $\varphi : R \rightarrow S, \exists! \varphi_a : R[x] \rightarrow S, r \mapsto \varphi(r), x \mapsto a$.

Def: kernel, ideal, principal ideal.

R is a field \Leftrightarrow only ideals of R are $\{0\}$ and R .

Def: Quotient Rings: R/I .

“First Isomorphism Theorem of Rings” R, R' rings, I ideal of $R, \varphi : R \rightarrow R'. I \subseteq \ker \varphi \Rightarrow \exists! \bar{\varphi} : R/I \rightarrow R'$ s/t $\bar{\varphi}(r + I) = \phi(r) \Rightarrow \bar{\varphi}(\pi(r)) = \varphi(r)$. Moreover, $\text{im}(\bar{\varphi}) = \text{im}(\varphi)$ and if $I = \ker \phi$, then $\bar{\varphi}$ is 1-1.

Cor: $\varphi : R \rightarrow R'$, then $R/\ker \varphi \cong \text{im} \varphi$.

“Adjoining” $\varphi : \frac{R[x]}{\langle p(x) \rangle} \rightarrow \tilde{R}$ given by $\varphi(x) = \alpha$ an isom., where \tilde{R} has a root of $p(x)$ at α .

Prop: R commie ring. $f(x) \in R[x], \deg f = n$. If $\text{LT}f(x) = ux^n, u \in R^\times$, every elt of $\frac{R[x]}{\langle f(x) \rangle}$ uniquely expressible as

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle f(x) \rangle, \text{ or } \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}, a_i \in R.$$

“Correspondence Thm for Quotient Rings” I ideal of R commie ring. 1-1 corr. “ideals of R that contain I ” \leftrightarrow “ideals of R/I ” Given by $I \subseteq J \subseteq R \mapsto J/I := \{j + i \mid j \in J\}, K \subseteq R/I \mapsto \{r \in R \mid r + I \in K\}$. Moreover, for J ,

$$R/I \Big/ J/I \cong R/J.$$

Def: Integral Domain: $ab = 0 \Rightarrow a = 0$ or $b = 0$. R ID $\Rightarrow R[x], R[x_1, \dots, x_n]$ ID.

Def: Field of Fractions: R ID, $F = \{\frac{a}{b} \mid a, b \in R, b \neq 0\}, \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.

Def: Maximal Ideal: R commie, $I \subset R$ ideal and $I \subseteq J \Rightarrow I = J$ or $J = R$.

“Hilbert’s Nullstellensatz” m max’l of $\mathbb{C}[x_1, \dots, x_n] \Rightarrow M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some ! $a_i \in \mathbb{C}$.

Def: Divides, Associates, GCD, LCM

Def: Irreducible: $b \neq 0, b \notin R^\times, b = ac \Rightarrow a \in R^\times$ or $a \in R^\times$.

Def: Prime: $b \mid ac \Rightarrow b \mid a$ or $b \mid c$.

Def: R Noetherian when Ascending Chain Condition holds for all ideals (not just principal).

Def: R UFD when ACC holds for principal ideals (factorizations exist) and factorizations unique up to units.

Prime implies irreducible in ID. Prime Equiv. to Irreducible in UFD.

Def: R is Principal Ideal Domain if R is ID and all ideals principal. PID implies UFD.

Def: R is Euclidean Domain if R an ID, $\exists \sigma : R \rightarrow \mathbb{N}$ so that $\forall f, g \in R, \exists q, r \in R, g = fq + r, \sigma(r) < \sigma(f)$ or $r = 0$.

ED implies PID implies UFD

Def: GCD g of a, b means $g \mid a, g \mid b$ and $d \mid a, d \mid b \Rightarrow d \mid g$.

Alg: Euclidean Algorithm.

Def: R UFD. $f(x) \in R[x]$ is primitive if GCD of coeff’s is 1_R .

Prop: R UFD, F FoF, $f(x) \in F[x], f(x) = c \cdot f_0(x), c \in F, f_0(x) \in R[x], f_0(x)$ primitive.

“Gauss’s Lemma” R UFD. $f(x), g(x) \in R[x]$. If f, g are primitive, so is their product.

Cor: $c(f(x)g(x)) = c(f(x))c(g(x))$.

Cor: $f(x)$ irred. in $R[x]$ iff either (1) $f(x)$ constant + irred. in R or (2) $f(x)$ primitive + irred. in $F[x]$.

Thm: R UFD. Every irred $f(x) \in R[x]$ is prime in $R[x]$

Prop: R ID, if R satisfies ACC for principal ideals, then $R[x]$ satisfies ACC for principal ideals.

Cor: R UFD, then $R[x], R[x_1, \dots, x_n]$ UFD (by Thm & Prop)

Lma: $f(x) \in \mathbb{Z}[x], p$ prime, $p \nmid \text{LT}(f(x))$. If $\bar{f}(x) \in \mathbb{Z}/p[x]$ irred, then $f(x) \in \mathbb{Q}[x]$ irred.

Lma: R ID, $p \in R, p \neq 0, p$ prime $\Leftrightarrow R/\langle p \rangle$ an ID.

“Eisenstein’s Criterion” R UFD, F FoF. $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$. $p \in R$ prime. If (1) $p \nmid a_n$ (2) $p \mid a_i, 1 \leq i < n$ (3) $p^2 \nmid a_0$ then $f(x)$ irred in $F[x]$. If $f(x)$ also primitive, then $f(x)$ irred. in $R[x]$.

Cor: Cyclotomic polynomial of prime-1 degree is irred in $\mathbb{Z}[x]$: $x^{p-1} + x^{p-2} + \cdots + x + 1$.

Def: Gauss Prime an irred. in $\mathbb{Z}[i]$.

Prop: p a Gauss Prime iff $x^2 - 1$ irred in $\mathbb{Z}/p[x]$ iff -1 is not a square mod p iff $p \equiv 3 \pmod{4}$.

Other Gauss Primes: $\pi = a + bi, a^2 + b^2 = p \in \mathbb{Z}$.

Def: R -Module, \mathbb{Z} -Module, free module, finitely generated, generating set, linear independent, basis.

Def: Module homomorphism, isomorphism, endomorphism, automorphism, quotient module.

“First Isomorphism Theorem of Modules” $\varphi : M \rightarrow N. \ker \varphi \subseteq M, \text{im} \varphi \subseteq N$ R -submods. $M/\ker \varphi \cong \text{im} \varphi$.

Derrick Stolee – Math 818 – Midterm Study Guide

Prop: M an R -mod is free of finite rank iff it has a basis.

Prop: M free R -mod with basis $B = \{b_1, \dots, b_n\}$. N any other R -mod, and choice of $y_1, \dots, y_n \in N$, $\exists! \varphi : M \rightarrow N, b_i \mapsto y_i$.

Prop: R commie. A $m \times n$ matrix an R mod isom $R^n \rightarrow R^m$ iff $n = m$ and $\det(A) \in R^\times$.

Thm: (R, σ) ED. Any $m \times n$ matrix A , $\exists P, Q$ elem. so that PAQ is diagonal with $d_1 \mid \dots \mid d_r$ (! up to units)

Cor: $A \in \text{GL}_n(R)$, $\exists P, Q$ elem. so that $PAQ = I_n$, $A = P^{-1}Q^{-1}$

Def: A presents M , presentation matrix.

Prop: R commie ring. A an $m \times n$ matrix. $M := R^m / \text{im}A$ and $x_i = \bar{e}_i$ then x_1, \dots, x_n generate M , $r_{1j}x_1 + \dots + r_{mj}x_m = 0$ and if $s_1x_1 + \dots + s_mx_m = 0$ then $\mathbf{s} \in \text{im}A$.

Prop: R commie ring, A $m \times n$ matrix. Then, following A' present same module $M = \frac{R^m}{\text{im}A}$.

1. $A' = QAP^{-1}$, $Q \in \text{GL}_m(R)$, $P \in \text{GL}_n(R)$.
2. A' obtained by deleting column of 0's (unless the last column)
3. j th column of A is e_i and A' is obtained by deleting the i th row of A .

For Exam 2:

Fundamental Theorem of Finitely Generated Modules over Euclidean Domains: Let R be an ED and F a finitely-generated R -module. Then,

$$M \cong R/\langle d_1 \rangle \oplus R/\langle d_2 \rangle \oplus \dots \oplus R/\langle d_k \rangle \oplus R^r$$

for some $k, r \geq 0$, $d_1, \dots, d_k \in R$ with $d_i \neq 0$ and $d_i \nmid R^\times \forall i$, and $d_1 \mid d_2 \mid \dots \mid d_k$. Moreover, k and r are unique and d_1, \dots, d_k are unique up to units.

Cor: Let M be a finitely generated abelian group. Then $M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r$ for $d_1, \dots, d_k \geq 2$, k, r, d_i are unique. If M is finite, $r = 0$ and hence, M is a direct sum of finite cyclic groups.

Cor: R an ED. M a finitely-generated R -module. Then $M \cong R/\langle p_1^{e_1} \rangle \oplus \dots \oplus R/\langle p_j^{e_j} \rangle \oplus R^r$ for some p_1, \dots, p_j prime in R , $e_1, \dots, e_j \geq 1$, $r \geq 0$. Moreover, this expression is unique up to units and ordering.

Prop: R a commie ring. The following are equivalent:

1. Every ideal of R is finitely-generated.
2. R has the ascending chain condition for all ideals.

Prop: If R is Noetherian, so is R/I for any ideal I .

Hilbert Basis Theorem: If R is Noetherian, so is $R[x_1, \dots, x_n]$.

Cor: If R is a field, or PID, then $\frac{R[x_1, \dots, x_n]}{I}$ is Noetherian for any n and any ideal I of $R[x_1, \dots, x_n]$.

Prop: R is commie Noetherian ring. If M is any finitely-generated R -module, then every submodule of M is also finitely generated.

Cor: Say R is Noetherian and M is finitely-generated, then M has a finite presentation matrix.

Relating Modules to Linear Transformations: Let A be an $n \times n$ matrix in a field F . We construct an $F[t]$ -module as follows: 1. $M = F^n$ as a group under $+$. 2. For $f(t) \in F[t]$, $\mathbf{v} \in M$ define $f(t)\mathbf{v} = f(A) \cdot \mathbf{v}$.

More generally, iff V any F -vector space, and $T : V \rightarrow V$ a linear operator, then let $V_T = V$ as a group under $+$ and define $f(t) \cdot \mathbf{v} = f(T)(\mathbf{v}) \forall f(t) \in F[t], \mathbf{v} \in V_T$.

Prop: For V_T As before, V_T is an $F[t]$ -module. Conversely, given an $F[t]$ -module M , we can view M as being an F -vector space via: $a \cdot m := a \cdot m$ (with right-side regarded as a constant polynomial in $F[t]$). Then multiplication by t on M is F -linear. Finally, these two constructions are mutual inverses:

$$\begin{aligned} (V, T) \in \{V, T : V \rightarrow V\} &\mapsto V_T \in \{F[t]\text{-modules}\} \\ M \in \{F[t]\text{-modules}\} &\mapsto (M, \text{mult. by } t) \in \{V, T : V \rightarrow V\} \end{aligned}$$

Def: If $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0$, the **companion matrix** of $f(t)$ is $C(f(t))$:

$$C(f(t)) := \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & 1 & & 0 & -a_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}$$

Derrick Stolee – Math 818 – Midterm Study Guide

Def: $\text{minpoly } A$ is the monic polynomial $f(t)$ of least degree satisfying $f(A) = 0$. Also, the ideal $\langle \text{minpoly } A \rangle$ is exactly the annihilator of the R -module V_A . If V_A is composed of a direct sum of finite cyclic groups such that each ideal generator divides the next as in

$$M \cong R/\langle f_1 \rangle \oplus R/\langle f_2 \rangle \oplus \cdots \oplus R/\langle f_k \rangle,$$

then $\text{minpoly } A = f_k(t)$. In this form, $\text{charpoly } A = \prod_{i=1}^k f_i(t)$.

[MISSING A BUNCH ON RCF HERE!!!!]

Thm: Let A be an $n \times n$ matrix with entries in F , a field. Let $M = F^n$, as an $F[t]$ -module. Then

$$F[t]^n \xrightarrow{tI_n - A} F[t]^n \rightarrow M \rightarrow 0$$

is a presentation of M , (ie: $M \cong \frac{F[t]^n}{\text{im}(tI_n - A)}$). Thus, to find the invariant factors of A , do row, column, and deletion operations to $tI_n - A$ to get

$$\begin{bmatrix} f_1(t) & 0 & \cdots \\ 0 & \ddots & \\ \vdots & & f_k(t) \\ 0 & \cdots & 0 \end{bmatrix}$$

with $f_1 \mid \cdots \mid f_k$, f_i non constant and monic. Then, f_1, \dots, f_k are the invariant factors of A .

Def: a **Jordan Block** is a $m \times m$ matrix $J_m(a)$:

$$J_k(a) := \begin{bmatrix} a & & & \\ 1 & a & & \\ & 1 & \ddots & \\ & & \ddots & a \\ & & & 1 & a \end{bmatrix}$$

Alg: To find the Jordan Canonical Form, follow these steps:

1. Find the roots of $\text{charpoly } A$.
2. Find their multiplicities. Determine the number of lin-indep eigenvectors for each root (dimension - rank for a single root).
3. If an ambiguous case, find $\text{minpoly } A$, and its exponent should help.

Existence of Jordan Canonical Form: Say A is an $n \times n$ matrix with entries in a field F . Assume $\text{charpoly}(A)$ factors completely into linear terms. That is, $\text{charpoly}(A) = (x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_l)^{m_l}$. Then,

$$A \sim \begin{bmatrix} J_{m_1}(a_1) & & & \\ & J_{m_2}(a_2) & & \\ & & \ddots & \\ & & & J_{m_l}(a_l) \end{bmatrix}$$

for some $l \geq 1$, $a_1, \dots, a_l \in F$, $m_1, \dots, m_l \geq 1$. Moreover, J is unique up to ordering of the $J_{m_i}(a_i)$'s.

Field Extensions

Def: $F \subseteq E$ is a *field extension* when F, E are fields.

Def: For any extension $F \subseteq E$, $\alpha \in E$ is *algebraic* in F if there exists $p(x) \in F[x]$ such that $p(\alpha) = 0$ when evaluated in E .

Def: For any extension $F \subseteq E$, $\alpha \in E$ is *transcendental* in F if there does not exist $p(x) \in F[x]$ such that $p(\alpha) = 0$ when evaluated in E .

Def: $F \subseteq E$, $\alpha \in E$ algebraic over F . $\{f(x) \in F[x] \mid f(\alpha) = 0\}$ is an ideal of $F[x]$. The *irreducible polynomial* of α over F is $\text{IrrPoly}_F(\alpha) :=$ the unique monic polynomial that generates this ideal.

Prop: $F \subseteq E$, $\alpha \in E$. Define $\varphi: F[x] \rightarrow E$ to be evaluation of $x = \alpha$: $\varphi(p(x)) = p(\alpha)$, and we have 1: $\text{im } \varphi = F[\alpha]$; 2. α is transcendental if $F \Leftrightarrow \varphi$ is one-to-one; 3. If α is algebraic over F , then $\ker \varphi = \langle \text{IrrPoly}_F(\alpha) \rangle$, $F[\alpha] = F(\alpha)$, and $\frac{F[x]}{\langle \text{IrrPoly}_F(\alpha) \rangle} \cong F[\alpha]$.

Cor: $F \subseteq E$, $\alpha, \beta \in E$, both algebraic over F . If $\text{IrrPoly}_F(\alpha) = \text{IrrPoly}_F(\beta)$, then there exists an isomorphism of fields $\theta: F[\alpha] \rightarrow F[\beta]$ so that $\theta(f) = f\forall f \in F$ and $\theta(\alpha) = \beta$. (Also known as a Galois Automorphism)

Derrick Stolee – Math 818 – Midterm Study Guide

Prop: $F \subseteq E, \alpha_1, \dots, \alpha_n \in E. F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n) \Leftrightarrow \alpha_1, \dots, \alpha_n$ are algebraic over F .

Def: The *degree* of a field extension $F \subseteq E$ is $[E : F] = \dim_F E$ as a vector space.

Prop: $F \subseteq E, \alpha \in E. [F(\alpha) : F] < \infty \Leftrightarrow \alpha$ is algebraic over F . In this case, $[F(\alpha) : F] = \deg \text{IrrPoly}_F(\alpha)$.

Degree Formula for Field Extensions: $F \subseteq E \subseteq L, [L : F] = [L : E][E : F]$.

Cor: $F \subseteq E, \alpha \in E$. If $[E : F] < \infty$, then α algebraic over F and $[F(\alpha) : F] \mid [E : F]$.

Cor: $F \subseteq E, \alpha, \beta \in E$. If α is algebraic over F and β algebraic over $F(\alpha)$, then β is algebraic over F .

Cor: $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}$ is a subfield of \mathbb{C} .

Cor: $F \subseteq E, [E : F] = p, p$ prime. There are no fields L properly contained in E and properly containing F . In other words, $E = F(\alpha)$ for any $\alpha \in E \setminus F$.

Cor: If $p(x) \in \mathbb{R}[x]$ is irreducible, then $\deg(p(x)) = 1$ or 2 .

Def: A field extension $F \subseteq E$ is *algebraic* if $\forall \alpha \in E, \alpha$ is algebraic.

Thm: Say $F \subseteq E \subseteq L. F \subseteq E$ and $E \subseteq L$ are both algebraic if and only if $F \subseteq L$ is algebraic.

Prop: Given a field F and a non-constant $p(x) \in F[x]$, there is a field extension $F \subseteq E$ so that $f(x)$ factors completely into linear factors in $E[x]$.

Def: F a field, $f(x) \in F[x], f(x) = a_n x^n + \dots + a_1 x + a_0$. The *derivative* is defined as $f'(x) := na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \dots + a_1$.

Prop: F a field, $f(x) \in F[x]$. There is an extension $F \subseteq E$ such that $f(x)$ has a double root in E if and only if $\gcd_{F[x]}(f(x), f'(x)) \neq 1$.

Prop: Say $p(x) \in F[x]$ is irreducible. $p(x)$ has a multiple root in some field extension $F \subseteq E$ if and only if $p'(x) = 0$.

Cor: If $\text{char } F = 0$ and $p(x) \in F[x]$ is irreducible, $p(x)$ does not have a multiple root in any extension of F .

Def: The *Freshman's Dream* is the following expansion in \mathbb{F}_p : $(x - \alpha)^p = x^p - \alpha^p$ (by Binomial Theorem).

Galois Theory: (assume every field F has $\text{char } F = 0$)

[Missed a bit]

Big Thm 1: $\#\text{Gal}(E/F) \mid [E : F]$.

Def: $F \subseteq E$ is Galois if $\#\text{Gal}(E/F) = [E : F]$

Def: Say $f(x) \in F[x]$. A *splitting field* of $f(x)$ over F is a field extension $F \subseteq E$ such that $f(x)$ factors completely into linear terms in $E[x]$ and $E = F(\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n \in E$ zeros of $f(x)$.

Big Thm 2: Let $F \subseteq E$ be any finite field extension with $\text{char } F = 0$. Then $F \subseteq E$ is Galois $\Leftrightarrow E$ is the splitting field over F for some $f(x) \in F[x]$.

Note: When $F \subseteq E$ is finite Galois, $E = F(\alpha_1, \dots, \alpha_n), n \mid [E : F] = \#\text{Gal}(E/F) \mid n!$.

Big Thm 3: $F \subseteq E$ is Galois \Leftrightarrow Whenever $\alpha \in E$, so is every root of $\text{IrrPoly}_F(\alpha)$.

Def: $E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha \forall \sigma \in G\}$.

Cor: By Definition, $F \subseteq E^G$, but $F \subseteq E$ Galois implies $F = E^G$.

Cor: Every finite field extension of F when $\text{char } F = 0$ is contained in a Galois extension.

Cor: If $F \subseteq E$ is finite Galois, and L is any intermediate field, then $L \subseteq E$ is finite Galois.

Main Thm of Galois Theory: Let $F \subseteq E$ be a finite Galois extension. Let $G := \text{Gal}(E/F)$. There is a bijection between

$$\begin{aligned} \{\text{subgroups of } G\} &\longleftrightarrow \{L \mid F \subseteq L \subseteq E\} \\ \text{Gal}(E/L) \leq G &\longleftarrow F \subseteq L \subseteq E \\ H \leq G &\longmapsto E^H := \{\alpha \in E \mid \sigma(\alpha) = \alpha \forall \sigma \in H\} \end{aligned}$$

Cor: For any $H \leq G, [G : H] = [E^H : F] = [E^H : E^G]$.

App: Find intermediate fields $F \subseteq L \subseteq E$ by subgroups of $\text{Gal}(E/F)$.

Cubic Polynomials: $f(x) = x^3 + ax^2 + bx + c \in F[x]$. Assume $f(x)$ irred. Let $E = F(\alpha_1, \alpha_2, \alpha_3)$. Then $[E : F] = 3$ or $6. \text{Gal}(E/F) \leq S_3, [F(\alpha_1) : F] = 3$. If $[E : F] = 3$, then $\text{Gal}(E/F) \cong A_3$, otherwise $\text{Gal}(E/F) \cong S_3$.

Def: Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, as above. The *discriminant* $D := \delta^2. D \in F$.

Prop: $\delta \in E^{\text{Gal}(E/F)} = F \Leftrightarrow \text{Gal}(E/F) \cong A_3 \Leftrightarrow D$ has a square root in F .

Formula for D : Let $f(x) = x^3 + ax^2 + bx + c$. Let $x = y - \frac{a}{3}$. $f(x) = f(y) = y^3 + py + q$.

Primitive Element Thm: Let $\text{char } F = 0. F \subseteq E$ any finite extension. The $E = F(\gamma)$ for some $\gamma \in E$.

Def: E any field. $\text{Aut}(E)$ the group of automorphisms of E . If $G \leq \text{Aut}(E)$, then define $E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha \forall \sigma \in G\}$.

Thm: $\text{char } E = 0, G \leq \text{Aut}(E), \#G = n < \infty$. Then $[E : E^G] = n$.

Lma: For all $\beta \in E$, let $\beta = \beta_1, \beta_2, \dots, \beta_m$ be the orbit of β under the action of G . Let $f(x) = (x - \beta_1) \cdots (x - \beta_m)$.

[Note: $m \mid n$ by LOIS] Then $f(x) \in F[x]$ and $f(x) = \text{IrrPoly}_F(\beta)$.

Cor: (Big Thm 1 is a corollary of this Thm)

Cor (*Artin's Thm*): E a field, $\text{char } E = 0, G \leq \text{Aut}(E), \#G < \infty$. Then $E^G \subseteq E$ is a Galois field extension and $\text{Gal}(E/E^G) = G$.

Derrick Stolee – Math 818 – Midterm Study Guide

Cor: Say E is a splitting field over F of an *irreducible* polynomial $f(x) \in F[x]$. Then $\text{Gal}(E/F)$ acts transitively on the roots of $f(x)$.

Prop: $F \subseteq E$ Galois. For a subgroup $H \leq G := \text{Gal}(E/F)$ and the corresponding intermediate field $L := E^H$: 1. $[G : H] = [L : F]$ and $H \trianglelefteq G$ if and only if $F \subseteq L$ is Galois. In this case, E is splitting field over F by a reducible polynomial $p(x) \in F[x]$ and L is splitting field over F by $g(x)|p(x) \in F[x]$, with $g(x)$ not constant. Also, for subgroup $H' \leq G$ and $L' := E^{H'}$, $H' = \sigma H \sigma^{-1}$ for some $\sigma \in G$ if and only if $L' = \sigma(L)$.

Def: Say $f(x) \in \mathbb{Q}[x]$. The roots of $f(x)$ are said to be *expressible by radicals* if there is a chain of field extensions

$$\mathbb{Q} \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \dots \subseteq E_n$$

so that all the roots of $f(x)$ are in E_n and E_{i+1} is the splitting field of $x^{n_i} - \gamma_i \in E_i[x]$ for some $n_i \geq 1$ and $\gamma_i \in E_i$.

Defr: A group G is *solvable* if there exists a chain of subgroups $H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$ and $\frac{H_{i+1}}{H_i}$ is an abelian group for all $0 \leq i < n$.

Prop: If E is the splitting field of $x^n - \gamma \in F[x]$ then $\text{Gal}(E/F)$ is a solvable group.

Thrm: $f(x) \in \mathbb{Q}[x]$, E the splitting field of $f(x)$ over \mathbb{Q} . The roots of $f(x)$ are expressible by radicals if and only if $\text{Gal}(E/\mathbb{Q})$ is solvable.

Claim: Say $f(x) \in \mathbb{Q}[x]$ is a fifth-degree irreducible polynomial so that $f(x)$ has exactly 3 real roots. $\text{Gal}(E/\mathbb{Q}) \cong S_5$ and thus the roots of $f(x)$ are not expressible by radicals.

Finite Fields:

Def: $\mathbb{F}_p = \mathbb{Z}/p$ where p is prime is a finite field.

Prop: For any prime p and any integer $n \geq 1$, there exists a field with $q = p^n$ elements.

Prop: Say E is a finite field of order $p^2 = q$, p prime, $n \geq 1$. Then, $E = \{\alpha \in E | f(\alpha) = 0\}$ where $f(x) = x^q - x$.

Exer: E^\times is a cyclic group.

Cor: If E and K are finite fields of the same order, then $E \cong K$.

Cor: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m | n$. In this case, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$.

Prop: Say p is prime, $q = p^n$, $n \geq 1$. $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic of order n and is generated by the Frobenius map:

$$\text{Frob} : \mathbb{F}_q \rightarrow \mathbb{F}_q, \text{Frob}(\alpha) = \alpha^p.$$