Theorems
Algebra qualifying course
MSU, Spring 2017

Joshua Ruiter

October 15, 2019

This document was made as a way to study the material from the spring semester algebra qualifying course at Michigan State University, in spring of 2017. It serves as a companion document to the "Definitions" review sheet for the same class.

Contents

1 Modules over Rings

1.1 Hom Functor

Theorem 1.1. *Let A be a ring and let*

$$X' \xrightarrow{f} X \xrightarrow{g} X'' \longrightarrow 0$$

be a sequence of A-modules. This sequence is exact if and only if, for every A-module Y, the the induced sequence

$$\mathrm{Hom}_A(X', Y) \xleftarrow{\mathrm{Hom}_A(f,Y)} \mathrm{Hom}_A(X, Y) \xleftarrow{\mathrm{Hom}_A(g,Y)} \mathrm{Hom}_A(X'', Y) \longleftarrow 0$$

is exact.

Theorem 1.2. *Let A be a ring and let*

$$0 \longrightarrow Y' \xrightarrow{f} Y \xrightarrow{g} Y''$$

be a sequence of A-modules. This sequence is exact if and only if, for every A-module X, the the induced sequence

$$0 \longrightarrow \mathrm{Hom}_A(X, Y') \xrightarrow{\mathrm{Hom}_A(X,f)} \mathrm{Hom}_A(X, Y) \xrightarrow{\mathrm{Hom}_A(X,g)} \mathrm{Hom}_A(X, Y'')$$

is exact.

1.2 Free Modules

Proposition 1.3 (Universal Property of Free Modules)**.** *Let M be a free module over a ring A, with basis $\{x_i\}_{i\in I}$. Let N be an A-module and $\{y_i\}_{i\in I}$ a subset of N. Then there is a unique homomorphism $\phi : M \to N$ so that $\phi(x_i) = y_i$ for all i.*

Proposition 1.4 (Mapping a Basis to a Basis is an Isomophism)**.** *Let M and N be free modules over a ring A with bases $\{x_i\}_{i\in I}$ and $\{y_i\}_{i\in I}$ respectively. Then the unique homomorphism $\phi : M \to N$ such that $\phi(x_i) = y_i$ is an isomorphism (of A-modules).*

Proposition 1.5. *Free A-modules with bases of equal cardinality are isomorphic (as A-modules).*

Proposition 1.6. *Let M be a free module over a ring A with basis $\{x_i\}_{i\in I}$. Then*

$$M \cong \bigoplus_{i\in I} Ax_i$$

(Note: $Ax_i = \{ax_i : a \in A\}$.)

Proposition 1.7. *Let M be a free module over a ring A with basis $\{x_i\}_{i\in I}$. Let $\mathfrak{a}$ be a two-sided ideal of A. Then $\mathfrak{a}M$ is a submodules of M, and $\mathfrak{a}x_i$ is a submodule of Ax_i. Then $Ax_i/\mathfrak{a}x_i \cong A/\mathfrak{a}$, and*

$$M/\mathfrak{a}M \cong \bigoplus_{i\in I} Ax_i/\mathfrak{a}x_i$$

That is, $M/\mathfrak{a}M$ is a free module over $A/\mathfrak{a}$ (free as an $A/\mathfrak{a}$ module).

Proposition 1.8. *Let M be a principal module over a commutative ring A, and let $x \in M$ so that $M = Ax$. Then the map $f : A \to M$ by $a \mapsto ax$ is a surjective A-module homomorphism. Let $\mathfrak{a} = \ker f$. Then $A/\mathfrak{a} \cong M$ as A-modules.*

Proposition 1.9. *Every free module is projective.*

1.3 Dual Module

Proposition 1.10. *Let E be a finite rank free module over a commutative ring A. (E has a finite basis.) Then $E^\vee$ is also free, with dimension equal to the dimension of E. In particular, given a basis $\{x_i\}_{i=1}^n$ of E, define $f_i : E \to A$ by $f_i(x_j) = \delta_{ij}$. Then $\{f_i\}_{i=1}^n$ is a basis of $E^\vee$.*

Proposition 1.11. *Let E be a finite rank free A-module. Then the map $E \mapsto E^{\vee\vee}$ defined by $x \mapsto (f \mapsto f(x))$ is an isomorphism (of A-modules).*

Proposition 1.12. *Let U, V, W be finite rank free modules over a commutative ring A, and let*

$$0 \longrightarrow W \xrightarrow{\lambda} V \xrightarrow{\phi} U \longrightarrow 0$$

be an exact sequence of A-modules. Then the induced sequence

$$0 \longrightarrow \operatorname{Hom}_A(U, A) \longrightarrow \operatorname{Hom}_A(V, A) \longrightarrow \operatorname{Hom}_A(W, A) \longrightarrow 0$$

(in other notation)

$$0 \longrightarrow U^\vee \longrightarrow V^\vee \longrightarrow W^\vee \longrightarrow 0$$

is exact.

1.4 Modules over Principal Ideal Domains

Proposition 1.13. *Let R be a principal ideal domain. Let F be a free R-module, and M a submodule of F. Then M is free, and its rank is less than or equal to the rank of F. (Note: It is very important that R is a PID. The result is not true when R is not a PID.)*

Proposition 1.14. *Let R be a PID, and let E be a finitely generated R-module. Then any submodule of E is finitely generated.*

Proposition 1.15. *Let R be PID, and let E, E' be R-modules such that E' is free. Let $f : E \to E'$ be a surjective homomorphism. Then there exists a free submodule F of E so that $f|_F : F \to E'$ is an isomorphism, and $E = F \oplus \ker f$.*

Proposition 1.16. *Let R be a PID, and let E be a finitely generated R-module. Then E/E_{tor} is free, and there is a submodule F of E so that $E = E_{\text{tor}} \oplus F$.*

Proposition 1.17 (Classification of Finitely Generated Modules over PIDs). *Let R be a PID and let E be a finitely generated R-module. Then E is a direct sum*

$$E = \bigoplus_p E(p)$$

where p ranges over a set of representative of associate classes of primes of R. Each $E(p)$ can be written as a direct sum

$$E(p) = R/(p^{k_1}) \oplus \ldots \oplus R/(p^{k_n})$$

where $1 \le k_1 \le \ldots \le k_n$. The sequence $k_1, \ldots, k_n$ is uniquely determined.

Proposition 1.18. *Let R be a PID and let E be a nonzero, finitely generated torsion R-module. Then E is isomorphic to a direct sum of non-zero factors*

$$E \cong R/(q_1) \oplus \ldots R/(q_n)$$

where $q_1, \ldots, q_n$ are non-zero non-units of R and $q_1|q_2|\ldots|q_n$. The sequence of ideals $(q_1), \ldots, (q_n)$ is uniquely determined by the above conditions.

Proposition 1.19 (Elementary Divisors Theorem)**.** *Let R be a PID and let F be a free R-module. Let $M \subset F$ be a nonzero finitely generated submodule. Then there exists a basis $\mathcal{B}$ of F and elements $\{e_1, \ldots, e_m\} \subset \mathcal{B}$ and non-zero elements $a_1, \ldots a_m \in R$ so that*

1. *The elements $a_1 e_1, \ldots, a_m e_m$ form a basis for M over R.*
2. *$a_i | a_{i+1}$ for $i = 1, \ldots, m-1$.*

The sequence of ideals $(a_1), \ldots, (a_m)$ is uniquely determined by the above.

1.5 Tensor Products

Proposition 1.20 (Generators for Tensor Product)**.** *Let R be a commutative ring and let $E_1, \ldots, E_n$ be R-modules. Then*

$$\{x_1 \otimes \ldots \otimes x_n : x_i \in E_i\}$$

is a generating set for $\bigotimes_{i=1}^n E_i$. That is, every element of $\bigotimes_{i=1}^n E_i$ can be written as

$$\sum_{i=1}^{n} r_i (x_1 \otimes \ldots \otimes x_n)$$

for $x_i \in E_i$ and $r_i \in R$.

Proposition 1.21 (Linearity of Tensor Product)**.** *Let R be a commutative ring and let X, Y be R-modules. Let $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ and $r \in R$. Then*

$$\begin{aligned} (x_1 + x_2) \otimes y_1 &= x_1 \otimes y_1 + x_2 \otimes y_1 \\ x_1 \otimes (y_1 + y_2) &= x_1 \otimes y_1 + x_1 \otimes y_2 \\ r(x_1 \otimes y_1) &= (r x_1) \otimes y_1 = x_1 \otimes (r y_1) \end{aligned}$$

(These properties generalize in the obvious way to a tensor product of more than two modules.)

Proposition 1.22 (Universal Property of Tensor Product)**.** *Let R be a commutative ring and let X, Y, G be R-modules. Then for every multilinear map $\phi : X \times Y \to G$, there is a unique R-module homomorphism $\phi_* : X \otimes_R Y \to G$ making the below diagram commute.*

$$\begin{array}{ccc} X \times Y & \xrightarrow{\otimes} & X \otimes_R Y \\ & \searrow^{\phi} & \downarrow{\scriptstyle \phi_*} \\ & & G \end{array}$$

That is, $\phi_*(x \otimes y) = \phi(x, y)$. (Note that this generalizes to tensor products of more than two modules.)

Proposition 1.23. *Let $m, n \in \mathbb{N}$ be relatively prime. Then viewing $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}$ modules, $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = 0$.*

Proposition 1.24 (Associativity of Tensor Product)**.** *Let E_1, E_2, E_3 be R-modules. There is a unique isomorphism $(E_1 \otimes E_2) \otimes E_3 \to E_1 \otimes (E_2 \otimes E_3)$ such that*

$$(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$$

Proposition 1.25 (Commutativity of Tensor Product)**.** *Let E, F be R-modules. There is a unique isomorphism $E \otimes F \to F \otimes E$ such that $x \otimes y \mapsto y \otimes x$.*

Proposition 1.26 (Functoriality of Tensor Product)**.** *Let $f_i : E_i' \to E_i$ for $i = 1, \ldots, n$ be a family of R-module homomorphisms. Then we get a map $\prod f_i : \prod E_i' \to \prod E_i$. Then the composition $\otimes \circ \prod f_i : \prod E_i' \to \bigotimes E_i$ induces a map $T : \bigotimes E_i' \to \bigotimes E_i$ by the universal property, and the following diagram commutes.*

$$\begin{array}{ccc} E_1' \times \ldots \times E_n' & \xrightarrow{\otimes} & E_1' \otimes \ldots \otimes E_n' \\ \downarrow{\scriptstyle \prod f_i} & & \downarrow{\scriptstyle T} \\ E_1 \times \ldots \times E_n & \xrightarrow{\otimes} & E_1 \otimes \ldots \otimes E_n \end{array}$$

The map T is sometimes notated as $T = f_1 \otimes \ldots \otimes f_n$.

Proposition 1.27. *Let R be a commutative ring and E, F, G be R-modules. Then $L(E, F; G) \cong L(E \otimes F, G)$. This isomorphism takes a bilinear map $f : E \times F \to G$ to the induced map $f_* : E \otimes F \to G$ where $f_*(e \otimes f) = f(e, f)$.*

Proposition 1.28. *Let R be a commutative ring and E, F, G be R-modules. Then $L(E, L(F, G)) \cong L(E, F; G)$. For $\phi : E \to L(F, G)$, this isomorphism is given by $\phi \mapsto f_\phi$ wher $f_\phi(x, y) = \phi(x)(y)$.*

Proposition 1.29 (Tensor Product Distributes over Direct Sum)**.** *Let $F, \{E_i\}_{i \in I}$ be R-modules. Then*

$$F \otimes \bigoplus_{i \in I} E_i \cong \bigoplus_{i \in I} (F \otimes E_i)$$

Proposition 1.30. *Let E be a free R-module with basis $\{v_i\}_{i \in I}$. Let F be an R-module. Then every element of $F \otimes E$ has a unique expression of the form*

$$\sum_{i \in I} y_i \otimes v_i$$

where $y_i \in F$ and only finitely many terms are nonzero.

Proposition 1.31. *Let E, F be free R-modules with respective bases $\{v_i\}_{i \in I}$ and $\{w_j\}_{j \in J}$. Then $E \otimes F$ is free with basis $\{v_i \otimes w_J\}$. As a result,*

$$\dim(E \times F) = (\dim E)(\dim F)$$

In particular, in the case where $F = R$, the tensor product $E \otimes R$ is isomorphic to E via the correspondence $x \mapsto x \otimes 1$.

Proposition 1.32. *Let E, F be finite dimensional free R-modules. Then there is a unique isomorphism*

$$\operatorname{End}_R(E) \otimes \operatorname{End}_R(F) \to \operatorname{End}_R(E \otimes F)$$

so that

$$f \otimes g \mapsto T(f, g)$$

Proposition 1.33 (Tensor Functor is Right Exact)**.** *Let*

$$0 \longrightarrow E' \xrightarrow{\ \phi\ } E \xrightarrow{\ \psi\ } E'' \longrightarrow 0$$

be an exact sequence of R-modules, and fix an R-module F. Then the sequence

$$F \otimes E' \longrightarrow F \otimes E \longrightarrow F \otimes E'' \longrightarrow 0$$

is exact. (When left exactness holds, F is called a ***flat*** *module.)*

Proposition 1.34. *Let R be a commutative ring with an ideal $\mathfrak{a}$. Let E be an R-module. Then the map $(R/\mathfrak{a}) \times E \to E/\mathfrak{a}E$ induced by*

$$(a, x) \mapsto ax \pmod{\mathfrak{a}E}$$

(where $a \in R$ and $x \in E$) is bilinear and induces an isomorphism

$$(R/\mathfrak{a}) \otimes E \cong E/\mathfrak{a}E$$

Proposition 1.35. *Let $m, n \in \mathbb{Z}$ and let $d = \gcd(m, n)$. Then*

$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$$

Proposition 1.36. *Let A be a nonzero finitely generated abelian group. Then $A \otimes_{\mathbb{Z}} A \neq 0$.*

Proposition 1.37. $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$. *(This is an example of a nonzero infinitely generated abelian group whose tensor product with itself is zero.)*

1.6 Flat Modules

Proposition 1.38. *Let F be an R module. The following are equivalent.*

1. *The functor $E \mapsto E \otimes F$ is exact.*
2. *The functor $E \mapsto E \otimes F$ is left exact.*
3. *For every injective R-module homomorphism $E' \to E$, the induced map $E' \otimes F \to E \otimes F$ is injective.*

(E, E' are R-modules and tensors are over R.)

Proposition 1.39. *Projective modules are flat.*

Proposition 1.40. *Let R be a commutative ring. Then R is flat as an R-module.*

Proposition 1.41. *Let R be a commutative ring and let $\{F_i\}_{i \in I}$ be a collection of R-modules. Then $\oplus_{i \in I} F_i$ is flat if and only if each F_i is flat.*

Proposition 1.42. *Let R be a principal ideal domain. Then an R-module F is flat if and only if it is torsion free.*

Proposition 1.43. *Let R be an integral domain, and let M be an R-module with torsion. Then M is not flat.*

Proposition 1.44. *Let R be a commutative ring and let F be an R-module. The following are equivalent:*

1. *F is flat.*
2. *$\mathrm{Tor}_1^R(F, M) = 0$ for every R-module M.*
3. *$\mathrm{Tor}_i^R(F, M) = 0$ for all $i \in \mathbb{N}$ and every R-module M.*
4. *$\mathrm{Tor}_1^R(F, R/I) = 0$ for all ideals $I \subset R$.*

Proposition 1.45. *Let F be a flat R-module and supppose that $0 \to N \to M \to F \to 0$ is an exact sequence of R-modules. Then for any R-module E, the sequence $0 \to N \otimes E \to M \otimes E \to F \otimes E \to 0$ is exact.*

Proposition 1.46. *Let R be a commutative ring, and let F be an R-module. Then F is flat if and only if for every ideal $I \subset R$ the natural map $I \otimes F \to IF$ given by $x \otimes f \to xf$ is an isomorphism.*

Proposition 1.47. *Let R be a commutative ring, and let F be an R-module. Then F is flat if and only if for every ideal $I \subset R$, the sequence $0 \to I \otimes F \to R \otimes F \to (R/I) \otimes F \to 0$ is exact.*

Guide to relationships between free, projective, and flat:
free $\implies$ projective $\implies$ flat
Over $\mathbb{Z}$, projective $\iff$ free
Over a PID, flat $\iff$ torsion free

1.7 Homology

Proposition 1.48. *Let R be a ring and let*

$$\dots \xrightarrow{d^{i-3}} E^{i-2} \xrightarrow{d^{i-2}} E^{i-1} \xrightarrow{d^{i-1}} E^{i} \xrightarrow{d^{i}} E^{i+1} \xrightarrow{d^{i+1}} \dots$$

be an exact sequence of R modules. Then for each i we have an exact sequence

$$0 \longrightarrow \ker d^i \longrightarrow E^i \xrightarrow{d^i} \operatorname{im} d^i \longrightarrow 0$$

Proposition 1.49. *Let R be a commutative ring and let M be an R-module. Then there is a free resolution of M.*

Proposition 1.50. *Let R be a ring and let E', E, E'' be chain complexes of R-modules, forming an exact sequence of morphisms of degree zero,*

$$0 \longrightarrow E' \xrightarrow{f} E \xrightarrow{g} E'' \longrightarrow 0$$

We can write this out fully as

$$\begin{array}{ccccccccc}
 & & \Big\downarrow{\scriptstyle d'_{i-2}} & & \Big\downarrow{\scriptstyle d_{i-2}} & & \Big\downarrow{\scriptstyle d''_{i-2}} & & \\
0 & \longrightarrow & E'_{i-1} & \xrightarrow{f_{i-1}} & E_{i-1} & \xrightarrow{g_{i-1}} & E''_{i-1} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle d'_{i-1}} & & \Big\downarrow{\scriptstyle d_{i-1}} & & \Big\downarrow{\scriptstyle d''_{i-1}} & & \\
0 & \longrightarrow & E'_{i} & \xrightarrow{f_{i}} & E_{i} & \xrightarrow{g_{i}} & E''_{i} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle d'_{i}} & & \Big\downarrow{\scriptstyle d_{i}} & & \Big\downarrow{\scriptstyle d''_{i}} & & \\
0 & \longrightarrow & E'_{i+1} & \xrightarrow{f_{i+1}} & E_{i+1} & \xrightarrow{g_{i+1}} & E_{i+1} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle d'_{i+1}} & & \Big\downarrow{\scriptstyle d_{i+1}} & & \Big\downarrow{\scriptstyle d''_{i+1}} & & \\
0 & \longrightarrow & E'_{i+2} & \xrightarrow{f_{i+2}} & E_{i+2} & \xrightarrow{g_{i+2}} & E''_{i+2} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle d'_{i+2}} & & \Big\downarrow{\scriptstyle d_{i+2}} & & \Big\downarrow{\scriptstyle d''_{i+2}} & &
\end{array}$$

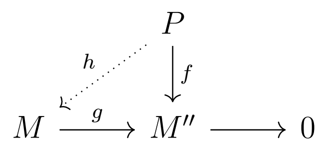
Then there exists a morphism $\delta : H(E'') \to H(E')$ of degree 1, that is, a family of morphisms $\delta_i : H_i(E'') \to H_{i+1}(E')$, fitting into the following long exact sequence:

$$\begin{aligned}
\dots \xrightarrow{\delta_{i-1}} H_i(E') \xrightarrow{H_i(f)} H_i(E) \xrightarrow{H_i(g)} H_i(E'') \xrightarrow{\delta_i} \\
\xrightarrow{\delta_i} H_{i+1}(E') \xrightarrow{H_{i+1}(f)} H_{i+1}(E) \xrightarrow{H_{i+1}(g)} H_{i+1}(E'') \xrightarrow{\delta_{i+1}} \dots
\end{aligned}$$

Proposition 1.51. *Let $f, g : E \to E'$ be homotopic morphisms of complexes. Then f, g induce the same homomorphism on homology, that is, $H(f_n) = H(g_n) : H_n(E) \to H_n(E')$.*

1.8 Projective Modules

Theorem 1.52. *Let A be a ring and let P be an A-module. The following are equivalent.*
(1) Given a homomorphism $f : P \to M''$ and a surjective homomorphism $g : M \to M''$, there exists a homomorphism $h : P \to M$ so that $g \circ h = f$. That is, given a commutative diagram as below, the dotted line can be filled in.



(2) Every exact sequence $0 \to M' \to M'' \to P \to 0$ splits.
(3) There exists a module M so that $P \oplus M$ is free.
(4) The functor $M \mapsto \operatorname{Hom}_A(P, M)$ is exact.

Proposition 1.53. *Let R be a ring and P be an R-module. The following are equivalent.*

1. *P is projective.*
2. *$\operatorname{Ext}^n_R(P, M) = 0$ for all R-modules M and $n \geq 1$.*
3. *$\operatorname{Ext}^1_R(P, M) = 0$ for all R-modules M.*

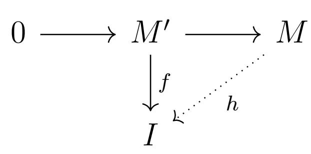
Proposition 1.54. *Every free module is projective.*

Proposition 1.55. *Over a PID, every projective module is free. (Thus over a PID, free is equivalent to projective.)*

Proposition 1.56. *Every projective module is flat.*

1.9 Injective Modules

Proposition 1.57. *Fix a ring R, and let I be an R-module. The following are equivalent.*
(1) Given an exact sequence $0 \to M' \to M$ of R-modules and a homomorphism $f : M' \to I$, there exists h so that the following diagram commutes.



(2) The functor $M \mapsto \operatorname{Hom}_R(M, I)$ is exact.
(3) Every exact sequence $0 \to I \to M \to M'' \to 0$ splits.

Proposition 1.58. *Let R be a ring and I be an R-module. The following are equivalent.*

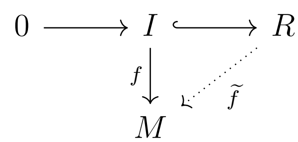
1. *I is injective.*
2. *$\operatorname{Ext}^n_R(M, I) = 0$ for all R-modules M and $n \geq 1$.*

3. $\text{Ext}^1_R(M, I) = 0$ *for all* R*-modules* M*.*

Proposition 1.59. *A product of injective modules is injective. Conversely, if a product of modules is injective, then each of the modules is injective.*

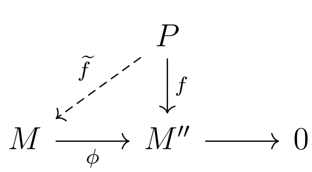
Proposition 1.60. *For* $\mathbb{Z}$ *modules, injective is equivalent to divisible.*

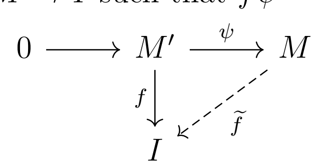
Proposition 1.61 (Baer's Criterion)**.** *Let* R *be a ring, and let* M *be an* R*-module. Then* M *is injective if and only if for every ideal* $I \subset R$ *and every* R*-linear map* $f : I \to M$*, we can find* $\widetilde{f} : R \to M$ *making the following diagram commute.*



1.10 Summary/Comparison of Injective/Projective R-modules

Projective	Injective
Submodules need NOT be projective	Submodules and quotient modules need NOT be injective
free $\implies$ projective over a PID, free $\iff$ projective projective $\implies$ flat	
	for $\mathbb{Z}$-modules, injective $\iff$ divisible for any ring, injective $\implies$ divisible
P is projective and $n \geq 1$ $\implies \forall M \ \operatorname{Ext}^n_R(P, M) = 0$	I is injective and $n \geq 1$ $\implies \forall M \ \operatorname{Ext}^n_R(M, I) = 0$
$\forall M \ \operatorname{Ext}^1_R(P, M) = 0$ $\implies P$ is projective	$\forall M \ \operatorname{Ext}^1_R(M, I) = 0$ $\implies I$ is injective
P is projective $\iff$ $\forall M, \forall n \geq 1 \ \operatorname{Ext}^n_R(P, M) = 0$	I is injective $\iff$ $\forall M, \forall n \geq 1 \ \operatorname{Ext}^n_R(M, I) = 0$
P is projective $\implies$ $M \mapsto \operatorname{Hom}_R(P, M)$ is exact	I is injective $\implies$ $M \mapsto \operatorname{Hom}_R(M, I)$ is exact
$0 \to M' \to M \to P \to 0$ aways splits	$0 \to I \to M \to M'' \to 0$ always splits
P is projective $\iff$ $\exists M$ such that $P \oplus M$ is free	Every module is a submodule of an injective module
P_1, P_2 are projective $\iff$ $P_1 \oplus P_2$ is projective	I_1, I_2 are injective $\iff$ $I_1 \oplus I_2$ is injective
If $\phi : M \to M''$ is surjective and $f : P \to M''$, then $\exists \widetilde{f} : P \to M$ such that $\phi \widetilde{f} = f$	If $\psi : M' \to M$ is injective and $f : M' \to I$, then $\exists \widetilde{f} : M \to I$ such that $\widetilde{f} \psi = f$





1.11 Ext and Tor

Proposition 1.62 (Computation of Tor)**.** *Let R be a ring, and let A, B be R-modules. Let*

$$\dots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

be a projective resolution of A. After we apply the functor $-\otimes_R B$ *and drop the term involving A, we get an induced chain complex*

$$\dots \longrightarrow P_2 \otimes_R B \longrightarrow P_1 \otimes_R B \longrightarrow P_0 \otimes_R B \longrightarrow 0$$

Then the homology of this sequence is $\mathrm{Tor}_n^R(A, B)$. *(The n-th homology occurs at the tensor involving* P_n*.)*

Proposition 1.63 (Computation of Ext)**.** *Let R be a ring, and let* A, B *be R-modules. Let*

$$\dots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

be a projective resolution of A. After we apply the functor $\mathrm{Hom}_R(-, B)$ *and drop the term involving A, we get an induced chain complex*

$$0 \longrightarrow \mathrm{Hom}_R(P_0, B) \longrightarrow \mathrm{Hom}_R(P_1, B) \longrightarrow \mathrm{Hom}_R(P_2, B) \longrightarrow \dots$$

(Note: The direction is reverse because $\mathrm{Hom}_R(-, B)$ *is contravariant.) Then the homology of this sequence is* $\mathrm{Ext}_n^R(A, B)$. *(The n-th homology occurs at the Hom involving* P_n*.)*

Proposition 1.64 (Symmetry of Tor)**.**

$$\mathrm{Tor}_n^R(A, B) \cong \mathrm{Tor}_n^R(B, A)$$

Proposition 1.65 ("Linearity" of Ext with Respect to Products)**.**

$$\mathrm{Ext}_R^n\left(\bigoplus_\alpha A_\alpha, B\right) \cong \prod_\alpha \mathrm{Ext}_R^n(A_\alpha, B)$$

$$\mathrm{Ext}_R^n(\left(A, \prod_\beta B_\beta\right) \cong \prod_\beta \mathrm{Ext}_R^n(A, B_\beta)$$

2 Field Theory

2.1 Review of Rings and Polynomials

Proposition 2.1. *Let R be an integral domain. Then* $R[x]$ *is an integral domain.*

Proposition 2.2. *Let k be a field. Then the polynomial ring* $k[x]$ *is a principal ideal domain.*

Proposition 2.3. *Let A be a commutative ring and* $I \subset A$ *an ideal. Then* A/I *is a field if and only if I is maximal.*

Proposition 2.4. *Let A be a commutative ring and* $I \subset A$ *an ideal. Then* A/I *is an integral domain if and only if I is prime.*

Proposition 2.5. *Let A be an integral domain. If* $a \in A$ *such that* $a \neq 0$ *and the principal ideal* $\langle a \rangle$ *is prime, then a is irreducible.*

Proposition 2.6. *Let A be a unique factorization domain. Then $p \in A$ is irreducible if and only if $\langle p \rangle$ is a prime ideal.*

Proposition 2.7 (Eisenstein's Criterion)**.** *Let R be a unique factorization domain, and let K be the quotient field of R. Let $f(x) = a_n x^n + \ldots + a_0 \in R[x]$ with degree $n \geq 1$. Let p be a prime in R such that*

$$p | a_0, a_1, \ldots a_{n-1} \qquad p \nmid a_n \qquad p^2 \nmid a_0$$

Then $f(x)$ is irreducible in $K[x]$.

Proposition 2.8 (Integral Root Test)**.** *Let R be a unique factorization domain with quotient field K. Let $f(x) = a_n x^n + \ldots + a_0 \in R[x]$. Let $\alpha \in K$ be a root of f, written as $\alpha = b/d$ where $b, d \in R$ and b, d are relatively prime. Then $b | a_0$ and $d | a_n$. In particular, if f is monic, then $\alpha = b$ so $\alpha \in R$ and $\alpha | a_0$. (Note: The most common application of this is when $R = \mathbb{Z}$ and $K = \mathbb{Q}$.)*

2.2 Algebraic Extensions

Proposition 2.9. *Every finite field extension is algebraic. That is, if E is a finite field extension of F, then every element of E is algebraic over F. (Note: Converse is false.)*

Proposition 2.10. *Let G, F, E be fields with $G \subset F \subset E$. Then*

$$[E : G] = [E : F][F : G]$$

In particular, if $\{x_i\}_{i \in I}$ is a basis for F over G and $\{y_j\}_{j \in J}$ is a basis for E over F, then $\{x_i y_j\}_{(i,j) \in I \times J}$ is a basis for E over G.

Proposition 2.11. *Let G, F, E be fields with $G \subset F \subset E$. Then E is a finite extension of G if and only if E is finite over F and F is finite over G.*

Proposition 2.12. *Let $k \subset E$ be a field extension and let α be algebraic over k. Then $k(\alpha) = k[\alpha]$ and $k(\alpha)$ is finite over k. Furthermore,*

$$[k(\alpha) : k] = \deg \operatorname{Irr}(\alpha, k)$$

That is, the degree of the field extension is equal to the degree of the minimal irreducible polynomial.

Proposition 2.13. *Let $k \subset E$ be a finite field extension. Then E is finitely generated over k.*

Proposition 2.14. *Let $k \subset E$ be a field extension, and suppose $E = k(\alpha_1, \ldots, \alpha_n)$. Let F be a field extension of E, so that $E, F \subset L$. Then $EF = F(\alpha_1, \ldots, \alpha_n)$.*

Proposition 2.15. *Let $E = k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension of a field k, and suppose that α_i is algebraic over k for each i. Then E is a finite and algebraic extension of k.*

Proposition 2.16. *The class of algebraic extensions is distinguished.*

Proposition 2.17. *The class of finite extensions is distinguished.*

Proposition 2.18. *The class of finitely generated extensions is distinguished. (Not proven in this class,)*

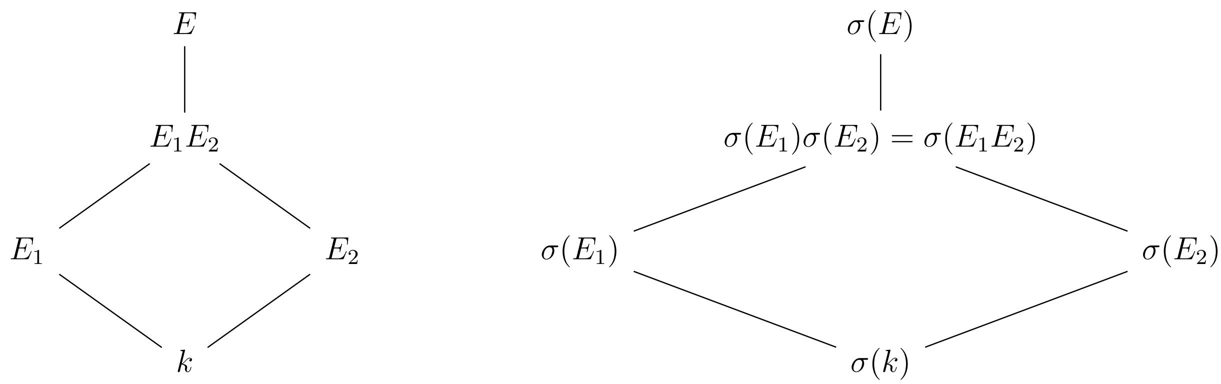
2.3 Algebraic Closure

Proposition 2.19. *Let k be a field, and $k \subset E$ be an algebraic extension. Let $\sigma : E \to E$ be an embedding of E into itself over k. (That is, $\sigma|_k = \mathrm{Id}_k$.) Then $\sigma : E \to E$ is an automorphism (that is, it is not merely injective, but also surjective.)*

Proposition 2.20. *Let k, E_1, E_2, E, L be fields with $k \subset E_1, E_2 \subset E$, and let $\sigma : E \to L$ be an embedding. Then*

$$\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$$

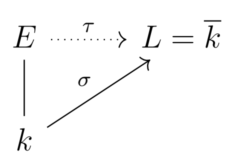
(The compositum of the images is the image of the compositum.)



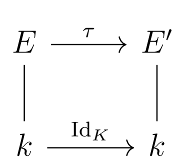
Proposition 2.21. *Let k be a field and $f \in k[x]$ of degree ≥ 1. Then there exists an extension E of k in which f has a root. (In particular, if f is irreducible we can choose the field $k[x]/(f)$.)*

Proposition 2.22. *Let k be a field. Then there exists an algebraically closed field $\overline{k}$ containing k as a subfield. Furthermore, the extension $k \subset \overline{k}$ is algebraic. (As will be shown later, this field is unique up to isomorphism.)*

Proposition 2.23. *Let k be a field and $k \subset E$ an algebraic extension, and $\sigma : k \to L$ an embedding of k into an algebraically closed field L. Then there exists an extension $\tau : E \to L$ so that $\tau|_k = \sigma$. If E is algebraically closed and L is algebraic over $\sigma(k)$, then τ is an isomorphism.*



Proposition 2.24. *Let k be a field and E, E' be algebraic extensions of k, with E, E' algebraically closed. Then there is an isomorphism $\tau : E \to E'$ such that $\tau|_k = \mathrm{Id}_k$.*

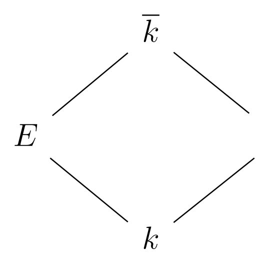


Proposition 2.25. *If k is an infinite field, then any algebraic extension of k has the same cardinality of k.*

Proposition 2.26. *If k is a finite field, then the algebraic closure of k is countably infinite. (No finite field is algebraically closed.)*

2.4 Splitting Fields and Normal Extensions

Proposition 2.27. *Let E, E' be splitting fields of $f \in k[x]$. Then there is an isomorphism $\tau : E \to E'$ such that $\tau|_k = k$. If $k \subset E \subset \overline{k}$, then any embedding $\phi : E' \to \overline{k}$ satisfying $\phi|_k = \mathrm{Id}_k$ is an isomorphism $\phi : E' \to E$.*

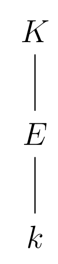


Proposition 2.28. *Let k be a field with algebraic closure $\overline{k}$. If we have a tower of algebraic extensions $k \subset K \subset \overline{k}$, then the following are equivalent:*

1. *K is the splitting field of a family of polynomials in $k[x]$.*
2. *Every embedding $\sigma : K \to \overline{k}$ is actually an isomorphism $\sigma : K \to K$. (That is, embeddings of splitting fields into the algebraic closure always map into the splitting field.)*
3. *Every irreducible polynomial in $k[x]$ that has a root in K splits into linear factors in K.*

(An extension satisfying the above is called normal.)

Proposition 2.29. *Normal extensions remain normal under lifting. That is, if $k \subset E \subset K$ and K is normal over k, then K is normal over E.*



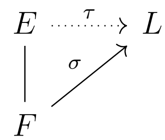
If K_1, K_2 are normal over k and $K_1, K_2 \subset L$, then the compositum K_1K_2 is normal over k, as is $K_1 \cap K_2$.

2.5 Separable Extensions

Proposition 2.30. *Let F, E, L be fields with L algebraically closed and $F \subset E$ and let $\sigma : F \to L$ be an embedding. Define*

$$S_\sigma = \{\tau : E \to L : \tau|_F = \sigma\}$$

That is, S_σ is the set of possible extensions of σ to E. Then the size of S_σ is independent of σ.



Proposition 2.31. *Let $k \subset F \subset E$ be a tower of fields. Then*

$$[E : k]_s = [E : F]_s [F : k]_s$$

Furthermore, if $[E : k]$ is finite, then $[E : k]_s$ is finite and

$$[E : k]_s \leq [E : k]$$

(Later we can show that $[E : k]_s$ divides $[E : k]$ whenever $[E : k]$ is finite.)

Proposition 2.32. *Let $k \subset F \subset E$ be a tower of fields with $[E : k]$ finite. Then*

$$[E : k]_s = [E : k] \iff [E : F]_s = [E : F] \text{ and } [F : k]_s = [F : k]$$

Proposition 2.33. *Let $k \subset F \subset K$ be a tower of fields and let $\alpha \in K$ be separable over k. Then α is separable over F.*

Proposition 2.34. *Let $k \subset E$ be a finite extension. Then E is separable over k if and only each $\alpha \in E$ is separable over k.*

Proposition 2.35. *Let $k \subset E$ be an algebraic extension, generated by $\{\alpha_i\}_{i \in I}$. If each α_i is separable over k, then E is separable over k.*

Proposition 2.36. *Separable extensions form a distinguished class.*

Proposition 2.37 (Primitive Element Theorem)**.** *Let $k \subset E$ be a finite extension. The following are equivalent:*

1. *There exists $\alpha \in E$ so that $E = k(\alpha)$.*

2. *There are only finitely many fields F such that $k \subset F \subset E$.*

If E is separable over k, then there exists $\alpha \in E$ such that $E = k(\alpha)$.

2.6 Finite Fields

Proposition 2.38. *If a field has q (finite) elements, then $q = p^n$ where p is a prime and $n \in \mathbb{N}$.*

Proposition 2.39. *For each prime p and each $n \in \mathbb{N}$, there exists a unique field F_{p^n} of order p^n. It is a subfield of the algebraic closure of $F_p = \mathbb{Z}/p\mathbb{Z}$. It is the splitting field of the polynomial*

$$f(x) = x^{p^n} - x$$

over F_p, and the elements of F_{p^n} are the roots of f. Every finite field is isomorphic to exactly one F_{p^n}.

Proposition 2.40. *Let F_q be a finite field (with q elements). Let $n \in \mathbb{N}$. In a given algebraic closure $\overline{F}_q$, there exists a unique extension of F_q of degree n, which is F_{q^n}.*

Proposition 2.41. *The multiplicative group of a finite field is cyclic.*

Proposition 2.42. *Let F_q be the finite field with $q = p^n$ elements. The group of automorphisms of F_q is cyclic of size n, and is generated by the Frobenius map $x \mapsto x^p$.*

Proposition 2.43. *Let p be prime and let $m, n \in \mathbb{N}$. In any algebraic closure of F_p, the subfield F_{p^n} is contained in F_{p^m} if and only if n divides m. When n divides m, F_{p^m} is a normal and separable extension of F_{p^n}, and the group of automorphisms of F_{p^m} over F_{p^n} is cyclic of order $\frac{m}{n}$, generated by ϕ^n. (ϕ is the Frobenius map.)*

2.7 Inseparable Extensions

Proposition 2.44. *Let k be a field with algebraic closure $\overline{k}$, and let $\alpha \in \overline{k}$. Let $f = \mathrm{Irr}(\alpha, k)$. If $\operatorname{char} k = 0$, then all roots of f have multiplicity one (f is separable). If $\operatorname{char} k = p$ for a prime p, then there exists $n \in \mathbb{N}$ so that every root of f has multiplicity p^n, and*

$$[k(\alpha) : k] = p^n [k(\alpha) : k]_s$$

and α^{p^n} is separable over k.

Proposition 2.45. *Let $k \subset E$ be a finite extension. Then the separable degree $[E : k]_s$ divides the degree $[E : k]$. We have*

$$\operatorname{char} k = 0 \implies \frac{[E:k]}{[E:k]_s} = 1$$
$$\operatorname{char} k = p \implies \frac{[E:k]}{[E:k]_s} = p^n \quad \text{for some } n \in \mathbb{N}$$

That is, every extension of a field of characteristic zero is separable.

2.8 Galois Theory

Proposition 2.46 (The Galois Correspondence)**.** *Let K be a finite Galois extension of k, with Galois group G. We define a map from the set of subgroups H of G to the set of subfields of K containing k by $H \mapsto K^H$ (where K^H is the fixed field of H). This is a bijection. Furthermore, K^H is Galois over k if and only if H is normal in G. If H is normal in G, then the map $G \to H$ by $\sigma \mapsto \sigma|_{K^H}$ induces an isomorphism of G/H to* $\mathrm{Gal}(K^H/k)$.

Proposition 2.47. *Let K be a Galois extension of k with Galois group G. Then $k = K^G$. If F is an intermediate field satisfying $k \subset F \subset K$, then K is Galois over F. Furthermore, the map*

$$F \mapsto \mathrm{Gal}(K/F)$$

from the set of intermediate fields to the set of subgroups of G is injective.

Proposition 2.48. *Let $k \subset K$ be a Galois extension with Galois group G. Let F, F' be intermediate fields ($k \subset F, F' \subset k$) and let H, H' be the subgroups of G belonging to F, F' respectively ($H = \mathrm{Gal}(K/F), H' = \mathrm{Gal}(K/F')$). Then*

1. *$H \cap H'$ belongs to FF' (that is, $H \cap H' = \mathrm{Gal}(K/FF')$).*
2. *The fixed field of the smallest subgroup of G containing H and H' is $F \cap F'$.*
3. *$F \subset F'$ if and only if $H' \subset H$ (the correspondence is inclusion reversing).*

Proposition 2.49. *Let E be a finite separable extension of k. Let K be the smallest normal extension of k containing E. Then K is finite Galois over k. There are only a finite number of intermediate fields F satisfying $k \subset F \subset E$.*

$$\begin{array}{c} K \\ | \\ E \\ | \\ F \\ | \\ k \end{array}$$

Proposition 2.50. *Let E be a algebraic separable extension of k, and suppose there exists $n \in \mathbb{N}$ so that every element of E as degree $\leq n$ over k. Then E is finite over k and $[E : k] \leq n$.*

Proposition 2.51 (Artin's Theorem)**.** *Let K be a field and let G be a finite group of automorphisms of K with $|G| = n$. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k, and $\mathrm{Gal}(K/k) = G$. Furthermore, $[K : k] = n$. That is, if K/k is a finite Galois extension, then $[K : k]$ is the size of the Galois group* $\mathrm{Gal}(K/k)$.

Proposition 2.52. *Let L/K be a finite Galois extension. Then the order of the Galois group of L over K is equal to the degree of the field extension $[L : K]$.*

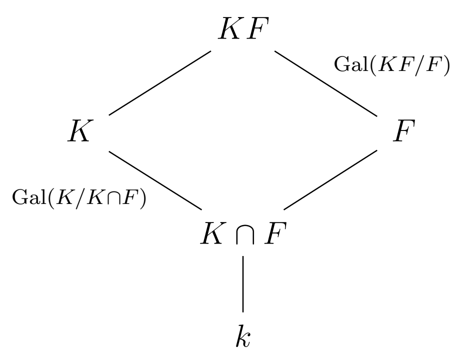
Proposition 2.53. *Let K be a finite Galois extension of k and let $G = \mathrm{Gal}(K/k)$. Then every subgroup H of G belongs to some subfield F so that $k \subset F \subset K$ (that is, $H = \mathrm{Gal}(K/F)$).*

Proposition 2.54. *Let K be a Galois extension of k with $\mathrm{Gal}(K/k) = G$. Let F be a subfield $k \subset F \subset K$, and let $H = \mathrm{Gal}(K/F)$. Then F is normal over k if and only if H is normal in G. If F is normal over k, then the restriction map $\mathrm{Gal}(K/k) \to \mathrm{Gal}(F/k)$ given by $\sigma \mapsto \sigma|_F$ is a homomorphism with kernel H. Thus*

$$\mathrm{Gal}(F/k) \cong \frac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/F)}$$

Proposition 2.55. *Let K/k be an abelian Galois extension. If F is an intermediate field $k \subset F \subset K$, then F is an abelian Galois extension of k. This same proposition holds true replacing "abelian" with "cyclic." (Normally, F/k may not even by Galois, but the corresponding subgroup is normal because the Galois group is abelian in this case.)*

Proposition 2.56 (Lifting of Galois Extensions)**.** *Let $k \subset K$ be a Galois extension and let $k \subset F$ be any extension, and suppose that K, F are contained in some field. Then $k \subset KF$ is Galois, and $K \cap F \subset K$ is Galois. Furthermore, the map $\mathrm{Gal}(KF/F) \to \mathrm{Gal}(K/K \cap F)$ given by $\sigma \mapsto \sigma|_K$ is an isomorphism.*

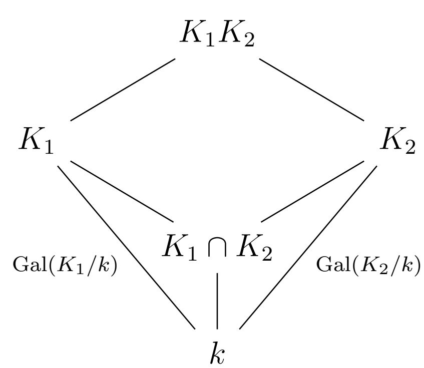


Proposition 2.57. *Let $k \subset K$ be a finite Galois extension. Let F be any extension of k. Then $[KF : F]$ divides $[K : k]$.*

Proposition 2.58. *Let K_1, K_2 be Galois extensions of k, where K_1, K_2 are contained in some field. Then the compositum K_1K_2 is Galois over k. Furthermore, the map*

$$\mathrm{Gal}(K_1K_2/k) \to \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k) \qquad \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is injective. If $K_1 \cap K_2 = k$, then it is an isomorphism.



Proposition 2.59. *Let K/k and L/k be abelian extensions of k, and K, L contained in some field. Then KL/k is an abelian extension.*

Proposition 2.60. *If K/k is an abelian extension, and E/k is any extension, then KE/k is an abelian extension.*

Proposition 2.61. *If K/k is an abelian extension, and $k \subset E \subset K$, then E/k is abelian and K/E is abelian.*

2.9 Computing Galois Groups of Polynomials

Proposition 2.62. *Let $f \in k[x]$ be a separable polynomial of degree n with Galois group G. Then the element of G permute the roots of f, so G embeds into S_n.*

Proposition 2.63 (Classification of Quadratic Extensions)**.** *Let k be a field of characteristic $\neq 2$. Let $f(x) = x^2 - a \in k[x]$, where a is not a square in k. Then f is separable and irreducible, and if α is a root in $\overline{k}$, then $k(\alpha)$ is the splitting field of f. Furthermore, the Galois group of f is cyclic of order 2.*

Proposition 2.64. *Let K/k be an extension of degree 2, with $\operatorname{char} k \neq 2$. Then there exists $a \in k$ such that $K = k(\alpha)$ and $\alpha^2 = a$.*

Proposition 2.65. *Let $f \in k[x]$ be a cubic. Then f can be written in the form $f(x) = x^3 + ax + b$ for $a, b \in k$. Concretely, given a general cubic*

$$ax^3 + bx^2 + cx + d$$

Make the subsitution $x = y - \frac{b}{3a}$ and get

$$y^3 + \left(\frac{3ac - b^2}{3a^2}\right) y + \left(\frac{2b^3 - 9abc + 27a^2 d}{27a^3}\right)$$

Note that since we just performed a linear substitution, the roots of the new cubic are just a linear shift of the roots of the original cubic. In particular, the Galois group remains the same.

Proposition 2.66 (Classification of Cubic Extensions)**.** *Let k be a field of characteristic $\neq 2, 3$, and let $f(x) = x^3 + ax + b \in k[x]$. Note that f is always separable, and that f is irreducible if and only if it has no root in k.*

Now assume f is irreducible, and let G be the Galois group. Then $G \cong S_3$ if and only if $\Delta(f)$ is a NOT square in k, and $G \cong \mathbb{Z}/3\mathbb{Z}$ otherwise (i.e. when the discriminant IS a square).

Proposition 2.67. *Let $f(x) = \mathbb{Q}[x]$ be irreducible with $\deg f = p$ for a prime p. If f has precisely two nonreal roots in $\mathbb{C}$, then the Galois group of f is S_p.*

Proposition 2.68. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial, and let p be a prime. Let $\overline{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ be the polynomial obtained by reducing the coefficients mod p. If $\overline{f}$ is separable, then there is a bijection between the roots of f and $\overline{f}$, and an embedding of the Galois group of $\overline{f}$ into the Galois group of f.*

In particular, if $\overline{f}$ factors as a product of irreducible polynomials of degree $n_1, \ldots, n_k$, then the Galois group of f contains an element that can be written as a product of disjoint cycles of length $n_1, \ldots, n_k$.

2.10 Roots of Unity

Proposition 2.69. *Let k be a field, and let n, m be relatively prime integers, not divisible by* $\operatorname{char} k$. *Let μ_n and μ_m be the cyclic groups of nth and mth roots of unity respectively. Then*

$$\mu_{mn} \cong \mu_n \times \mu_m$$

Proposition 2.70. *Let k be a field, and $n \in \mathbb{N}$ not divisible by* $\operatorname{char} k$. *Let ζ_n be a primitive nth root of unity in $\overline{k}$. Then $k(\zeta_n)/k$ is a cyclic Galois extension, of order d where $d|n$.*

Proposition 2.71. *Let ζ be a primitive nth root of unity over $\mathbb{Q}$. Then*

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$$

where ϕ is the Euler totient function. Furthermore, we have an isomorphism

$$\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Proposition 2.72. *Let $n, m \in \mathbb{N}$ be relatively prime. Let ζ_n, ζ_m be primitive nth and mth roots of unity respectively. Then*

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$$

Proposition 2.73. *Let ζ_p be a primitive pth root of unity, and define*

$$S = \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) \zeta_p^v$$

Then

$$S^2 = \left(\frac{-1}{p}\right) p$$

Consequently, every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Proposition 2.74 (Artin). *Let G be a monoid and k a field. Let $\chi_1, \ldots, \chi_n : G \to k^\times$ be distinct characters. Then they are linearly independent (over k).*

Proposition 2.75. *Let k be a field and $\alpha_1, \ldots, \alpha_n$ be distinct elements of $k^\times$. If*

$$\sum_i a_i \alpha_i^m = 0$$

for all $m \in \mathbb{N}$, then $a_i = 0$ for all i. (Note: To prove this, apply the previous theorem to the characters $m \mapsto \alpha_i^m$ from $\mathbb{Z}_{\geq 0}$ to $k^\times$.)

2.11 Norm and Trace

Proposition 2.76 (Properties of Norm)**.** *Let E/k be a finite extension. Then the norm $N_{E/k}$ is a multiplicative homomorphism $E^\times \to k^\times$. If $k \subset F \subset E$ is a tower of finite extensions, then*

$$N_k^E = N_k^F \circ N_F^E$$

If $E = k(\alpha)$ and $f(x) = \operatorname{Irr}(\alpha, k) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, then

$$N_k^{k(\alpha)} = (-1)^n a_0$$

Proposition 2.77 (Properties of Trace)**.** *Let E/k be a finite extension. Then the trace $\operatorname{Tr}_{E/k}$ is an additive homomorphism $E \to k$. If $k \subset F \subset E$ is a tower of finite extensions, then*

$$\operatorname{Tr}_k^E = \operatorname{Tr}_k^F \circ \operatorname{Tr}_F^E$$

If $E = k(\alpha)$ and $f(x) = \operatorname{Irr}(\alpha, k) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, then

$$\operatorname{Tr}_k^{k(\alpha)}(\alpha) = -a_{n-1}$$

Proposition 2.78 (Linear Map/Matrix Interpretation of Norm and Trace)**.** *Let E/k be a finite extension. For $\alpha \in E$, define $m_\alpha : E \to E$ by $x \mapsto \alpha x$. Viewing E as a finite dimensional k-vector space, m_α is a linear map. Then*

$$N_k^E(\alpha) = \det(m_\alpha) \qquad \operatorname{Tr}_k^E(\alpha) = \operatorname{Tr}(m_\alpha)$$

Proposition 2.79. *Let E/k be a finite separable extension. Then the map $E \times E \to k$ given by*

$$(x, y) \mapsto \operatorname{Tr}(xy)$$

is a bilinear pairing. Furthermore, if we define $\operatorname{Tr}_x : E \to k$ by $\operatorname{Tr}_x(y) = \operatorname{Tr}(xy)$, then the map $E \to E^\wedge$ given by $x \mapsto \operatorname{Tr}_x$ is an isomorphism.

Proposition 2.80. *Let E/k be a finite separable extension, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of E into $\overline{k}$ over k. Let $w_1, \ldots, w_n$ be a basis of E over k. Then the vectors*

$$\xi_i = (\sigma_i(w_1), \ldots, \sigma_i(w_n)) \qquad i = 1, \ldots, n$$

are linearly independent over E.

Proposition 2.81 (Hilbert's Theorem 90)**.** *Let K/k be a cyclic Galois extension of degree n, with Galois group $G = \langle \sigma \rangle$. Let $\beta \in K$. Then $N_k^K(\beta) = 1$ if and only if there exists $\alpha \neq 0$ in K such that $\beta = \frac{\alpha}{\sigma(\alpha)}$.*

Proposition 2.82 (Kummer)**.** *Let k be a field, and let $n \in \mathbb{N}$ with $\gcd(n, \operatorname{char} k) = 1$ (if $\operatorname{char} k \neq 0$). Assume that there is a primitive nth root of unity in k.*

1. *Let K/k be a cyclic Galois extension of degree n. Then there exists $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies the equation $x^n - a = 0$ for some $a \in k$.*

2. *If $a \in k$ and α is a root of $x^n - a$, then $k(\alpha)/k$ is a cyclic Galois extension of degree d where $d|n$, and $\alpha^d \in k$.*

Proposition 2.83 (Hilber's Theorem 90, Additive Form)**.** *Let K/k be a cyclic Galois extension of degree n with Galois group $G = \langle\sigma\rangle$. Let $\beta \in K$. Then $\mathrm{Tr}_k^K(\beta) = 0$ if and only if there exists $\alpha \in K$ such that $\beta = \alpha - \sigma(\alpha)$.*

Proposition 2.84 (Artin-Schreier)**.** *Let k be a field of characteristic $p > 0$.*

1. *If K/k is a cyclic Galois extension of degree p, then there exists $\alpha \in K$ such that $K = k(\alpha)$ and α satisfies the equation $x^n - x - a = 0$ for some $a \in k$.*

2. *If $a \in k$, then the polynomial $x^n - x - a$ either has one root in k or is irreducible. If it has a root in k, then all roots lie in k. If it is irreducible, then $k(\alpha)/k$ is a cyclic Galois extension of degree p.*

2.12 Solvable and Solvable by Radicals

Proposition 2.85. *Solvable extensions form a distinguished class.*

Proposition 2.86. *Extensions that are solvable by radicals form a distinguished class.*

Proposition 2.87. *Let E/k be a finite separable extension. Then E/k is solvable by radicals if and only if it is solvable.*