Fields.Know

Uncultured Tramp

October 20, 2016

Contents

1 Basic Definitions

$\texttt{Field} ::? \sum k : \texttt{Set} \, . \, (k \times k \to k) \times (k \times k \to k)$
$(k, \cdot, +) : \texttt{Abelean} \iff (k, +), (k \setminus \{0_+\}, \cdot) : \texttt{Abelean} \wedge (k, \cdot, +) : \texttt{CommutativeRing}$

$\texttt{implicit} :: \texttt{Field} \to \texttt{Set}$
$\texttt{implicit}(k, \cdot, +) := k$

$\texttt{division} :: \prod k : \texttt{Field} \, . \, k \to (k \setminus \{0\}) \to k$
$\texttt{division}(0, a) = 0/a := 0$
$\texttt{division}(b, a) = b/a := ba^{-1}$

$\texttt{Subfield} :: \prod K : \texttt{Field} \, . \, ?\texttt{Field}$
$k : \texttt{Subfield} \iff \exists \texttt{Mono}_{\mathsf{RING}}(k, K)$

$\texttt{Extension} :: \prod K : \texttt{Field} \, . \, ?\texttt{Field}$
$k : \texttt{Extension} \iff \exists \texttt{Mono}_{\mathsf{RING}}(K, k)$

2 Polynomials over a Field

2.1 Polynomials as functions

$$\texttt{implicit} :: \prod k : \texttt{Field} \,.\, k[\mathbb{Z}_+] \to k \to k$$

$$\texttt{implicit}(p)(x) := \sum_{i=0}^{\deg p} a_i x^i$$

$$\texttt{implicit} :: \prod k : \texttt{Field} \,.\, \prod n \in \mathbb{N} \,.\, k[\mathbb{Z}_+^n] \to k^n \to k$$

$$\texttt{implicit}(p)(x) := \sum_{\alpha \in \operatorname{multideg} p} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$$

$\texttt{ZeroPolinomial} :: \forall L : \texttt{Field} \,.\, \forall F : \texttt{Subfield}(L) : \#F \geq \aleph_0 \,.\, \forall p \in L[\mathbb{Z}_+^n] \,.$
$\quad .\, p_{|F} =_{F^n \to F} 0 \Rightarrow p =_{L[\mathbb{Z}_+^n]} 0$

Proof $-$

Assume $x \in F$,

$$0 = p(x) = \sum_{\alpha \in \operatorname{multideg} p} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} = \sum_{\alpha \in \operatorname{multideg} p} \sum_{k=1}^{d} l_{i,\alpha} e_i \prod_{i=1}^{n} x_i^{\alpha_i} = \sum_{k=1}^{d} \left(\sum_{\alpha \in \operatorname{multideg} p} l_{i,\alpha} \prod_{i=1}^{n} x_i^{\alpha_i} \right) e_i$$

$$e_i : \texttt{LinearlyIndependant} \rightsquigarrow \forall i \in d \,.\, \sum_{\alpha \in \operatorname{multideg} p} l_{i,\alpha} \prod_{i=1}^{n} x_i^{\alpha_i} = 0;$$

$$\forall x \in F \,.\, \forall i \in d \,.\, \sum_{\alpha \in \operatorname{multideg} p} l_{i,\alpha} \prod_{i=1}^{n} x_i^{\alpha_i} = 0 \rightsquigarrow l = 0 \rightsquigarrow p = 0$$

$\square$

2.2 Divisibility

$\texttt{CommonDivisor} :: \prod k : \texttt{Field} \; . \; k[\mathbb{Z}_+] \times k[\mathbb{Z}_+] \to ?\texttt{Monic}(k)$
$p : \texttt{CommonDivisor}(a, b) \iff p|a \wedge p|b$

$\texttt{GCD} :: \prod k : \texttt{Field} \; . \; \prod a, b \in k[\mathbb{Z}_+] \; . \; ?\texttt{CommonDivisor}(a, b)$
$\texttt{GCD} := \arg\max \deg p$

$\texttt{UniqueGCD} :: \forall k : \texttt{Field} \; . \; \forall a, b \in k[\mathbb{Z}_+] \; . \; \exists! \texttt{GCD}(a, b)$
Proof $\approx$

As k is field $k[x]$ is principle domain, so $(a, b) = (p)$ for some p which can be taken to be monic without loss of generality as k is a field again. So $\texttt{CommonDivisor}(a, b)$ exists. Assume we take any other common divisor q but then, since $p = xa + yb$ and hence $q|p$, q has lower degree than p. This proofs that $p : \texttt{GCD}(a, b)$

Now assume $p, q : \texttt{GCD}(a, b)$. We know that $\deg p = \deg q$ and that $\text{lc}(p) = \text{lc}(q) = 1$. If $p \neq q$ then their least common denominator will have higher degree and still be a common divisor, which leads to contradiction with initial hypothesis. This proves $p = q$ and hence uniqueness.
□

$\texttt{gcd} :: \prod k : \texttt{Field} \; . \; k[\mathbb{Z}_+] \times k[\mathbb{Z}_+] \to k[\mathbb{Z}_+]$
$\texttt{gcd}(a, b) := \gcd(a, b) := \texttt{UniqueGCD}(k)(a, b) \; \texttt{Extract}$

$\texttt{GCDFieldInvariant} :: \forall k : \texttt{Field} \; . \; \forall K : \texttt{Subfield}(k) \; . \; \forall a, b \in K[\mathbb{Z}_+] \; . \; \gcd_k(a, b) \in K[\mathbb{Z}_+]$
Proof $\approx$
$\gcd_K(a, b) \in K[\mathbb{Z}_+]$ exists and is $\texttt{GCD}(k)$, as $\gcd_K(a, b) \in (a, b)_k$ and hence divisible by $\gcd_k(a, b)$. Moreover, $\texttt{GCD}(k)$ is unique so it must be the case that $\gcd_K(a, b) = \gcd_k(a, b) \in K[\mathbb{Z}_+]$.
□

$\texttt{RelativelyPrime} :: \prod k : \texttt{Field} \; . \; ?(k[\mathbb{Z}_+] \times k[\mathbb{Z}_+])$
$(a, b) : \texttt{RelativelyPrime} \iff \gcd(a, b) = 0$

$\texttt{RLFieldInvariant} :: \forall k : \texttt{Field} \; . \; \forall K : \texttt{Subfield}(k) \; . \; \forall (a, b) : \texttt{RelativelyPrime}(K) \; . \; (a, b) : \texttt{RelativelyPrime}(k) \; .$
Proof $\approx$
Application of $\texttt{GCDFieldInvariant}$
□

2.3 Roots

$\texttt{Root} :: \prod k : \texttt{Field} \; . \; k[\mathbb{Z}_+] \to ?k$
$x : \texttt{Root}(p) \iff p(x) = 0$

$\texttt{RootExtension} :: \forall k : \texttt{Field} \; . \; \forall p \in k[\mathbb{Z}_+] : \deg p > 0 \; . \; \exists K : \texttt{Extension}(k) : \exists \texttt{Root}(K)(p)$
Proof $\approx$
p has roots in k, otherwise it is irreducible in $k[\mathbb{Z}_+]$. Assume second alternative, as first is trivial. By Ring theory, as p is irreducible,

$$K := \frac{k[\mathbb{Z}_+]}{(p)} : \texttt{Field}$$

with trivial monomorphism $f : k \to K$ such that $f : x \mapsto x \mod p$, hence a superfield of k. Now take $a = [0, 1] \mod p \in K$, then $p(a) = p \mod p = 0$ which means that a is a root of p in K.
$\square$

$\texttt{Splits} : \prod k : \texttt{Field} \; . \; ?k[\mathbb{Z}_+]$
$p : \texttt{Splits} \iff \exists n \in \mathbb{N} : \exists f : n \to k[\mathbb{Z}_+] : \forall i \in n \; . \; \deg f \leq 1 : p = \prod_{i=1}^{n} f_i$

$\texttt{SplittingExtension} :: \forall k : \texttt{Field} \; . \; \forall p \in k[\mathbb{Z}_+] \; . \; \exists K : \texttt{Extension}(k) : (f : \texttt{Splits}(K))$
Proof $\approx$
Corollary of RootsExtension.
$\square$

$\texttt{RPInExtension} :: \forall k : \texttt{Field} \; . \; \forall p, q \in k[\mathbb{Z}_+] \; . \; (p, q) : \texttt{RelativelyPrime}(k) \iff \forall K : \texttt{Extension}(k) \; . \; (p, q) : \texttt{RelativelyPrime}(K)$
Proof $\approx$
Corollary of RootsExtension.
$\square$

$\texttt{RPIrreducable} :: \forall k : \texttt{Field} \; . \; \forall (p, q) : \texttt{Irreducable}(k[\mathbb{Z}_+]) : p \neq q \; . \; \forall K : \texttt{Extension}(k) \; . \; (p, q) : \texttt{RelativelyPrime}(K)$
Proof $\approx$
Corollary of RootsExtension.
$\square$

$\texttt{SplittingField} : \prod k : \texttt{Field} \; . \; \texttt{Finite}(k[\mathbb{Z}_+]) \to ?\texttt{Extension}(k)$
$\texttt{SplittingField}(P) := \min\{K : \texttt{Extension}(k) : \forall p \in P \; . \; p : \texttt{Splits}(K)\}$

$\texttt{SplittingFieldExists} :: \forall k : \texttt{Field} \; . \; \forall P : \texttt{Finite}(k[\mathbb{Z}_+]) \; . \; \exists \texttt{SplittingField}(P)$
Proof $\approx$
Take splitting Field for $\prod P$.
$\square$

$\texttt{Algebraic} :: \prod k : \texttt{Field} \; . \; \prod K : \texttt{Extension}(k) \; . \; ?K$
$a : \texttt{Algebraic} \iff a \in \mathcal{A}(k, K) \iff \exists p \in k[\mathbb{Z}_+] : p(a) = 0$

$\texttt{Transcedental} :: \prod k : \texttt{Field} \ . \ \prod K : \texttt{Extension}(k) \ . \ ?K$
$a : \texttt{Transcedental} \iff a \in \mathcal{T}(k, K) \iff a \, ! \, \mathcal{A}(k, K)$

$\texttt{Minimal} :: \prod k : \texttt{Field} \ . \ \prod K : \texttt{Extension}(k) \ . \ \mathcal{A}(k, K) \rightarrow ?\texttt{Monic}$
$\texttt{Minimal}(a) := \arg\min\{\deg p | p \in k[\mathbb{Z}_+] : p(a) = 0\}$

$\texttt{MinimalExists} :: \forall k : \texttt{Field} \ . \ \forall K : \texttt{Extension}(k) \ . \ \forall a \in \mathcal{A}(k, K) \ . \ \exists! \texttt{Minimal}(a)$
Proof $\approx$
Set in definition of Minimal polynomial is will be an ideal of $k[\mathbb{Z}_+]$, so as $k[\mathbb{Z}_+]$ is a principle domain it will have a unique monic generator p. p is minimal.
$\square$

$\texttt{minimal} :: \prod k : \texttt{Field} \ . \ \prod K : \texttt{Extension}(k) \ . \ \prod a \in \mathcal{A}(k, K) \ . \ \texttt{Minimal}(a)$
$\texttt{minimal} = \mathrm{minimal}(a) := \texttt{MinimalExists}(k)(K)(a) \ \texttt{Extract}$

$\texttt{Conjugate} :: \prod k : \texttt{Field} \ . \ \prod K : \texttt{Extension}(k) \ . \ ?(\mathcal{A}(k, K) \times \mathcal{A}(k, K))$
$(a, b) : \texttt{Conjugate} \iff \mathrm{minimal}(a) = \mathrm{minimal}(b)$

$\texttt{multiplicity} :: \prod k : \texttt{Field} \ . \ \prod p \in k[\mathbb{Z}_+] \ . \ \texttt{Root}(p) \rightarrow \mathbb{N}$
$\texttt{multiplicity}(a) := \mathrm{mult}(p, a) := \max\left\{n \in \mathbb{N} : [-a, 1]^n \;\middle|\; p\right\}$

$\texttt{SimpleRoot} :: \prod k : \texttt{Field} \ . \ \prod p \in k[\mathbb{Z}_+] \ . \ ?\texttt{Root}(p)$
$a : \texttt{SimpleRoot} \iff \mathrm{mult}(p, a) = 1$

$\texttt{MultipleRoot} :: \prod k : \texttt{Field} \ . \ \prod p \in k[\mathbb{Z}_+] \ . \ ?\texttt{Root}(p)$
$a : \texttt{MultipleRoot} \iff \mathrm{mult}(p, a) > 1$

$\texttt{Separable} :: \prod k : \texttt{Field} \ . \ ?\texttt{Irreducible}(k[\mathbb{Z}_+])$
$p : \texttt{Separable} \iff \forall K : \texttt{Extension}(k) \ . \ \forall a : \texttt{Root}(K)(p) \ . \ a : \texttt{SimpleRoot}(K)(p)$

$\texttt{SimpleRootsCriterion} :: \forall k \in \texttt{Field} \ . \ \forall p \in k[\mathbb{Z}_+] \ . \ \big(\forall a : \texttt{Root}(p) \ . \ a : \texttt{SimpleRoot} \iff (p, p') : \texttt{RelativelyPrime}\big)$
Proof $\approx$

Assume all roots are simple. By $\texttt{RLFieldInvariant}$ we can work in splitting field of f. Then

$$p(x) = \prod_{i=1}^{n}(x - a_i) \quad p'(x) = \sum_{j=1}^{n} \frac{1}{x - a_j} \prod_{i=1}^{n}(x - a_i)$$

and from the structure of p' using the fact that $a_i \neq a_j$ for $i \neq j$ we see that it indeed coprime with p.

Now assume that p and p' are coprime. Also assume that $\mathrm{mult}(a_1) > 1$, then

$$p'(x) = (x - a_1) \sum_{j=1}^{n} \frac{1}{(x - a_j)(x - a_1)} \prod_{i=1}^{n}(x - a_i)$$

which is not coprime with p, hence a contradiction.
$\square$

$\texttt{SeparabilityCriterion} :: \forall k : \texttt{Field} . \forall p : \texttt{Irreducible}(k[\mathbb{Z}_+]) . p : \texttt{Separable} \iff p' \neq_{k\to k} 0$
Proof $\approx$

assume that p is separable which implies that she has only simple roots in her splitting field . As p is irreducable it is not constant, so $p' \neq 0$. By previous theorem we can see that p' has no common roots with p is not zero as a function.

Now consider that p' is not a zero . If p and p' is not coprime then $p' \in k[\mathbb{Z}_+]$ and has all repeated roots with multiplicity reduced by one . So $g = \gcd(p, p')$ have $\deg g > 0$. And by $\texttt{GCDFieldInvariant}$ g also belongs to $k[\mathbb{N}_+]$ which means that $p$is not irreducable, a contradiction.

□

$\texttt{IrreducableAreSeparableChar0} :: \forall k : \texttt{Field} : \mathrm{char}(k) = 0 . \forall p : \texttt{Irreducible}(k[\mathbb{Z}_+]) . p : \texttt{Separable}$
Proof $\approx$
As p is not a constant her derivative is not 0 and hence is not a zero function.

□

$\texttt{IrreducableInseparableCharN} :: \forall n \in \mathbb{N} . \forall k : \mathrm{char}(k) = n . \forall p : \texttt{Irreducible}(k[\mathbb{Z}_+]) .$
$. p\, !\, \texttt{Separable} \iff \exists f : \texttt{Separable} \exists d \in \mathbb{N} : p(x) = f\left(x^{p^d}\right)$
Proof $\approx$

Assume that p is inseparable, then $p' = 0$. This means that all coefficients of f' are divisible by n. On the over hand we know that coefficients of p cannot be divisible by n which means that $p(x) = (x^{p^d})$ for some f and d. By taking maximal possible d we must get separable as it will have at least one monomial with exponent coprime with n

The inverse proof is obvious

□

$\texttt{InseparableCharNMultiplicity} :: \forall n \in \mathbb{N} . \forall k : \mathrm{char}(k) = n . p\, !\, \texttt{Separable} . \exists d \in \mathbb{N} : \forall a : \texttt{Root}(p) . \mathrm{mult}(p) = n^d$
Proof $\approx$
By previous theorem we know that over splitting field we will have:

$$p(x) = f\left(x^{p^d}\right) = \prod_{i=1}^{N}\left(x^{p^d} - a_i\right) = \prod_{i=1}^{N}\left(x^{p^d} - b_i^{p^d}\right) = \prod_{i=1}^{N}(x - b_i)^{p^d}$$

□

$\texttt{radicalExponent} :: \prod n \in \mathbb{N} . \prod k : \texttt{Field} : \mathrm{char} k = p . !\texttt{Separable} \to \mathbb{N}$
$\texttt{radicalExponent}(p) = d(p) := \texttt{IrreducableInseparableCharN}(n)(k)_2\ \texttt{Extract}$

$\texttt{FFIsSeparable} :: \forall n \in \mathbb{N} . \forall k : \mathrm{char}(k) = n : \#k < \aleph_0 . \forall p : \texttt{Irreducible}(k) . p : \texttt{Separable}$
Assume p is inseparable . Note that $\#k = n^m$ for some m. So multiplicative group of k has order $n^m - 1$ so for every $a \in k$ $a^{n^m} = a$. So for every a, $a = b^n$ for some $b = a^{n^{m-1}}$. so

$$p(x) = \sum_{i=0}^{d} a_i x^{ip} = \sum_{i=0}^{d} b_i^p x^{ip} = \left(\sum_{i=0}^{d} b_i x^i\right)^p$$

which is reducible in k which means contradiction.

2.4 Tests of Irreducibility

`LoalizationTHM` :: $\forall R$: `Ring` . $\forall k$: `Field` . $\forall \sigma$: $\mathcal{M}_{\mathsf{RING}}(R, F)$. $\forall p \in R[\mathbb{Z}_+]$. $\deg(p^\sigma) = \deg(p) \wedge p^\sigma$: `Irreducible`$(k) \Rightarrow p$: `DegreewiseIrreducible`(R)
Proof $\approx$

Assume that p is reducible over R. Then write $p = fg$. But with this factorization $p^\sigma = f^\sigma g^\sigma$ which means that means that p^σ is also reducible as $\deg f^\sigma, \deg g^\sigma > 0$, a contradiction. $\square$

`LoalizationRule` :: $\forall R : PID$. $\forall a$: `Prime`(R) . $\forall p \in R[\mathbb{Z}_+] : a \not| \mathrm{lc}(p)$. $\pi_a p$: `Irreducible`$(k) \Rightarrow$ p : `DegreewiseIrreducible`(R)
Proof $\approx$

$\frac{R}{(a)}$ is a field and by hypothesis degree was not reduced. $\square$

`EisenstinCriterion` :: $\forall R$: `IntegralDomain` . $\forall p \in R[\mathbb{Z}_+]$.
. $\forall a$: `Prime`$(R) : a \not| \mathrm{lc}(p) : a^2 \not| p_0 : \forall i \in \deg p - 1 \,.\, a|p$. p : `DegreewiseIrreducible`
Proof $\approx$
Assume that p is degree-wise reducible. Write $p = fg$ and apply projection

$$pi_a(\mathrm{lc}(p))x^{\deg p} = \pi_a p = (\pi_a f)(\pi_a g)$$

This means that all coefficients of f,g are 0 expect the leading ones but at least one of them must have non-zero constant part which gives us a contradiction.
$\square$

2.5 Reciprocal Polynomials

3 Field Extension

3.1 Lattice of Extensions

$\texttt{degree} :: \prod k : \texttt{Field} \,.\, \texttt{Extension}(k) \to \mathbb{N}_\infty$
$\texttt{degree}(k) = [K : k] := \dim_k K$

$\texttt{Tower} :: ?[\,]|\texttt{Field} \times \texttt{Tower}$
$(A, (B, T)) : \texttt{Tower} \iff A : \texttt{Subfield}(B)$

$\texttt{TowerDegree} :: \forall [A, B, C] : \texttt{Tower} \,.\, [C : A] = [C : B][B : A]$
Proof $\approx$
Use basis decomposition $\square$

$\texttt{composite} : \prod K : \texttt{Field} \,.\, \texttt{Subfield}(K) \times \texttt{Subfield}(K) \to \texttt{Subfield}(K)$
$\texttt{composite}(A, B) := \min\{k : \texttt{Subfield}(K) : A, B \subset k\}$

$\texttt{composite} : \prod K : \texttt{Field} \,.\, \texttt{Set}\,\texttt{Subfield}(K) \to \texttt{Subfield}(K)$
$\texttt{composite}(\mathcal{E}) = \bigvee \mathcal{E} := \min\{k : \texttt{Subfield}(K) : \forall E \in \mathcal{E} \,.\, E \subset k\}$

$\texttt{extensionLattice} :: \texttt{Field} \to \texttt{Lattice}$
$\texttt{extensionLattice}(K) = \mathfrak{L}(K) := \big(\texttt{Subfield}(K), \subset, \cap, \texttt{composite}\big)$

3.2 Types of Extensions

$\texttt{Algebraic} :: \prod k : \texttt{Field} \, . \, ?\texttt{Extension}(k)$
$K : \texttt{Algebraic} \iff \forall a \in K \, . \, a \in \mathcal{A}(k)$

$\texttt{NormalExtension} :: \prod k : \texttt{Field} \, . \, ?\texttt{Extension}(k)$
$K : \texttt{NormalExtension} \iff \exists P : \texttt{Set}\, k[\mathbb{Z}_+] : K = \min\{F : \texttt{Extension}(k) : \forall p \in P \, . \, p : \texttt{Splits}(F)\}$

$\texttt{Transcendental} := !\, \texttt{Algebraic}$

$\texttt{extend} :: \prod K : \texttt{Field} \, . \, \texttt{Subfield}(K) \to K \to \texttt{Subfield}(K)$
$\texttt{extend}(k)(a) = k(a) := \min\{F : \texttt{Extension}(k) : a \in F\}$

$\texttt{extendWithSet} :: \prod K : \texttt{Field} \, . \, \texttt{Subfield}(K) \to \texttt{Set}(K) \to \texttt{Subfield}(K)$
$\texttt{extend}(k)(A) = k(A) := \min\{F : \texttt{Extension}(k) : A \subset F\}$

$\texttt{FinitelyGeneratedExtension} :: \prod k : \texttt{Field} \, . \, ?\texttt{Extension}(k)$
$K : \texttt{FinitelyGeneratedExtension} \iff \exists A : \texttt{Finite}(K) : K = k(A)$

$\texttt{SimpleExtension} :: \prod k : \texttt{Field} \, . \, ?\texttt{Extension}(k)$
$K : \texttt{SimpleExtension} \iff \exists a \in K : K = k(a)$

$\texttt{PrimitiveElement} :: \prod k : \texttt{Field} \, . \, \prod K : \texttt{SimpleExtension}(k) \, . \, ?K$
$a : \texttt{PrimitiveElement} \iff K(a)$

$\texttt{FiniteExtension} :: \prod k : \texttt{Field} \, . \, ?\texttt{Extension}(k)$
$K : \texttt{FiniteExtension} \iff [K : k] < \infty$

$\texttt{SeparableElement} :: \prod k : \texttt{Field} \, . \, ?\mathcal{A}(k)$
$a : \texttt{SeparableElement} \iff \mathrm{minimal}(a) : \texttt{Separable}(k)$

$\texttt{SeparableExtension} :: \prod k : \texttt{Field} \, . \, ?\texttt{Algebraic}(k)$
$K : \texttt{SeparableExtension} \iff \forall a \in K \, . \, a : \texttt{SeparableElement}(k)$

$\texttt{GaloisExtension} := \texttt{SeparableExtension} \,\&\, \texttt{NormalExtension}$

3.3 Distinguished Extension

$\texttt{2-Tower} :: ?\texttt{Tower}$
$T : \texttt{2-Tower} \iff \operatorname{len}(T) = 3$

$\texttt{lowerStep} :: \texttt{2-Tower} \to \texttt{Field}$
$\texttt{lowerStep}[A, B, C] := A$

$\texttt{upperStep} :: \texttt{2-Tower} \to \texttt{Field}$
$\texttt{upperStep}[A, B, C] := C$

$\texttt{intermidiateField} :: \texttt{2-Tower} \to \texttt{Field}$
$\texttt{intermidiateField}[A, B, C] := B$

$\texttt{ExtensionSystem} :=? \sum k : \texttt{Field} \,.\, \texttt{Extension}(k)$

$\texttt{TowerProperty} :: ?\texttt{ExtensionSystem}$
$X : \texttt{TowerProperty} \iff \forall [A, B, C] : \texttt{2-Tower} \,.\, \big((A, B), (B, C) \in X \iff (A, C) \in X\big)$

$\texttt{LiftingProperty} :: ?\texttt{ExtensionSystem}$
$X : \texttt{LiftingProperty} \iff \forall (A, B) \,.\, \forall K : \texttt{Extension}(A) \,.\, (K, B \vee K) \in X$

$\texttt{CompositionClosure} :: ?\texttt{ExtensionSystem}$
$X : \texttt{CompositionClosure} \iff \forall (A, B), (A, C) \,.\, (K, B \vee C) \in X$

$\texttt{Distinguished} := \texttt{TowerProperty} \,\&\, \texttt{LiftingProperty} \,\&\, \texttt{CompositionClosure}$

$\texttt{FinitelyGeneratedExtension} : \texttt{Distinguished}$
$\texttt{Proof} \ =$
$\texttt{Assume}\ [A, B, C] : 2 - \texttt{Tower},$
$\texttt{Assume}\ (A, B), (B, C) : \texttt{FinitelyGeneratedExtension},$
$a := \eth\texttt{FinitelyGeneratedExtension}(A, B) : \texttt{Finite}(B) : B = A(a),$
$b := \eth\texttt{FinitelyGeneratedExtension}(B, C) : \texttt{Finite}(C) : C = B(b),$
$c := a \cup b : \texttt{Finite}(C),$
$X := A(c) : \texttt{FinitelyGeneratedExtension}(A),$
$(1) := \eth\texttt{FinitelyGeneratedExtension}(A)(X, B, C) : X = C,$
$=E(1, \eth(A, X)) : ((A, C) : \texttt{FinitelyGeneratedExtension});$
$\texttt{Assume}\ (A, C) : \texttt{FinitelyGeneratedExtension},$
$c := \eth\texttt{FinitelyGeneratedExtension}(A, B) : \texttt{Finite}(B) : C = A(c),$
$(1) := \eth\texttt{FinitelyGeneratedExtension}(V)(A, B, C, c)B(c) = C,$

3.4 Simple extensions[?]

SimpleAlgebraicExtensionIso :: $\forall k : \texttt{Field} \; . \; \forall a \in \mathcal{A}(k) \; . \; \frac{k}{(\text{minimal}(a))} \cong_{\mathsf{RING}} k(a)$
Proof $\approx$

$$\frac{k}{(\text{minimal}(a))} =_{\texttt{Set}} \{p \in k[\mathbb{Z}_+] : \deg p < \deg \text{minimal}(a)\}$$

As minimal polynomial $m = \text{minimal}(a)$ is irreducible, and each p in quotient has lower degree p and m will be coprime. So if $p \neq 0$ there are two polynomials a,b such that

$$ap = ap + bm \mod m = 1$$

So our quotient is a field with $a = p^{-1}$. To see that our structures are indeed isomorphic we construct a map $\nu : p(x) \mapsto p(a)$. By results stated above ν is indeed an isomorphism of rings. $\square$

DegreeOfSimpleExtension :: $\forall k : \texttt{Field} \; . \; \forall a \in \mathcal{A}(k) \; . \; [k : k(a)] = \deg \text{minimal}(a)$
Proof $\approx$
write minimal polimomial as $x^d - p(x)$ with $d = \deg \text{minimal}(a)$ so there is a relation $a^d = p(a)$ on $k(a)$. Which means that there is a basis in $k(a)$:

$$1, a, \dots, a^{d-1}$$

so $\dim_k k(a) = d$. $\square$

ConjugatesAreIso :: $\forall k : \texttt{Field} \; . \; \forall a, b : \texttt{Conjugate}(k) \; . \; k(a) \cong_{\mathsf{RING}} k(b)$
Proof $\approx$
From DegreeOfSimpleExtension it follows that $\dim k(a) = \dim k(b)$ so $k(a) \cong_{\mathsf{VS}(k)} k(b)$ by properties of finite dimensional vector space. However linear isomorphism $\nu : p(a) \mapsto p(b)$ still will be an isomorphism of rings as it preserves multiplication with same substitution rule arising from minimal polynomial. So $k(a) \cong_{\mathsf{RING}} k(b)$. $\square$

SimpleAlgIsAlg :: $\forall k : \texttt{Field} \; . \; \forall a : \mathcal{A}(k) \; . \; k(a) : \texttt{Algebraic}$
Proof $\approx$
let K be an algebraic closure of k. Then any polynomial $p(a)$ of $a \in K$ is also in K, Hence is algebraic. $\square$.

SimpleAlgIsFinite :: $\forall k : \texttt{Field} \; . \; \forall a : \mathcal{A}(k) \; . \; k(a) : \texttt{FiniteExtension}$
Proof $\approx$
It is known that from DegreeOfSimpleExtension $[k : k(a)] = \deg \text{minimal}(a) < \infty$. Result follows. $\square$.

SimpleFiniteIsAlg :: $\forall k : \texttt{Field} \; . \; \forall K : \texttt{Extension}(k) \; . \; \forall a \in K : (k(a) : \texttt{FiniteExtension}) \; . \; a \in \mathcal{A}(k)$
Proof $\approx$
$k(a)$ will have a basis as a VectorSpace (k) of form $(a^k)_{k=0}^d$. Finiteness of a implies that for some $n \in \mathbb{N}$ we have relation $a^n = p(a)$ for some $p \in k[\mathbb{Z}_+] : \deg p < n$. But this means that a is a root of $x^n - p(x)$, hence algebraic. $\square$

`SimpleAlgChracterization` :: $\forall k : \texttt{Field} \; . \; \forall A : \texttt{Finite}\, \mathcal{A}(k) \; . \; \big(\exists a \in \mathcal{A}(k) : k(A) \cong_{\mathsf{RING}} k(a) \iff \#(\{F : \texttt{Field} : k <_{\mathsf{RING}} F <_{\mathsf{RING}} k(A)\}/\cong_{\mathsf{RING}}) < \aleph_0\big)$
Proof $\approx$

Assume $k(A) \cong_{\mathsf{RING}} k(\alpha)$ for some $\alpha \in \mathcal{A}(k)$. Then $\infty > d = [k(a) : k] = [k(A) : k]$. So There is a finite basis of $k(A)$ of form $E = (a_{n_i}^{m_i})_{i=1}^{d}$ consisting of elements of A. for any distinct a_j we will have distinct extension of k, namely $k(a_j)$, we will have different extensions of k such that $k <_{\mathsf{RING}} k(a_j) <_{\mathsf{RING}} k(A)$. And so on for all finite combinations $k(a_{i_1}, a_{i_2}, \dots, a_{i_j})$. As d is finite where can be only finite amount of differnt combinations up to isomorphism.

Now assume that number of intermediate fields is finite. Take an arbitrary element $a \in A : a \notin k$. We will apply finite induction. If $k(a) \cong k(A)$ then we are done. Now assume that we know that $k(\alpha) \cong k(a, \dots, a_j)$ and $k(\alpha)(\beta) \cong k(A)$. We will need to show that there exists γ such that $k(\gamma) = k(A)$. If k is finite. Then multiplicative group $k(A)$ still finite so it is cyclic implying there exists a generating element γ, hence $k(\gamma) = k(A)$ and we are done. If $\#k \geq \aleph_0$, let $\gamma = \alpha + a\beta$ with $1 \neq a \neq 0$. As there only finite amount of fields in-between k and $k(A)$ where mus exist $b \neq a$ such that $k(\alpha + a\beta) \cong k(\alpha + b\beta)$. This implies that $\alpha, \beta \in k(\gamma)$ so $k(\gamma) \cong k(A)$. Induction implies that there must some γ such that $k(\gamma) = k(A)$. $\square$

`InfSimpleAlgChracterization` :: $\forall k : \texttt{Field} : \#k \geq \aleph_0 \; . \; \forall n \in \mathbb{N} \; . \; \forall a \in \mathcal{A}^n(k) \; . \; \exists v \in k^n : k(\{a\}) = k(\langle a, v \rangle)$
Proof $\approx$
Corollary for `SimpleFiniteIsAlg` in infinite case. $\square$

`SimpleTransExtension` :: $\forall k : \texttt{Field} \; . \; \forall r \in \mathcal{T}(k) \; . \; k(r) \cong_{\mathsf{RING}} k(\mathbb{Z}_+)$

`TransExtensionThm` :: $\forall k : \texttt{Field} \; . \; \forall r \in \mathcal{T}(k) \; . \; \forall f, g : \texttt{RelativelyPrime}(k[\mathbb{Z}_+]) \; .$
$. \; f(r)/g(r) \in \mathcal{T}(k) \wedge k(r) : \texttt{Algebraic}\,(k(f(t)/g(t)))$

3.5 Algebraic Extension and Closure[?]

$\texttt{FiniteIsAlg} :: \forall k : \texttt{Field} \,.\, \forall K : \texttt{FiniteExtension}(k) \,.\, K : \texttt{Algebraic}(k)$

$\texttt{Algebraic} : \texttt{Distinguished}$

$\texttt{AlgebraiclyClosed} :: ?\texttt{Field}$
$k : \texttt{AlgebraiclyClosed} \iff \forall p \in k[\mathbb{Z}_+] \,.\, p : \texttt{Splits}(k)$

$\texttt{AlgebraicClosure}(k) := \texttt{AlgebraicalyClosed} \,\&\, \texttt{Algebraic}(k)$

$\texttt{ClosureExists} :: \forall k : \texttt{Field} \,.\, \exists! K : \texttt{Extension} \,\&\, \texttt{AlgebraicalyClosed}$

$\texttt{algebraicClosure} :: \prod k : \texttt{Field} \,.\, \texttt{AlgebraicClosure}(k)$
$\texttt{algebraicClosure} = \overline{k} := \texttt{ClosureExists}(k)$

$\texttt{AlgebraicAreField} :: \forall k : \texttt{Field} \,.\, \mathcal{A}(k) : \texttt{Field}$

3.6 Extensions of Embeddings[?]

$\texttt{EmbedingExtension} :: \prod k, F : \texttt{Field} \ . \ \prod K : \texttt{Extension}(k) \ . \ (k \hookrightarrow F) \to ?(K \hookrightarrow F)$
$S : \texttt{EmbedingExtension} \iff S \in \mathrm{Homm}_\sigma(K, G) \iff S_{|k} = \sigma$

$\texttt{AutTHM} :: \forall k : \texttt{Field} \ . \ \forall K : \texttt{Extension}(k) \ . \ \mathrm{Homm}_{\mathrm{id}_{k,K}}(K, K) = \mathrm{Aut}_{\mathsf{ALG}(k)} K$

$\texttt{simpleExtension} :: \prod k, K : \texttt{Field} \ . \ \prod a \in \mathcal{A}(k) \ .$
$. \ \texttt{Root}(K, \mathrm{minimal}(a)) \to (k \hookrightarrow K) \to k(a) \hookrightarrow K$
$\texttt{simpleExtension}(b, \sigma) = \sigma_b := \Lambda f(a) \in k \ . \ f^\sigma(b)$

$\texttt{SimpleEmbeddingExtension} :: \forall k, K : \texttt{Field} \ . \ \forall a \in \mathcal{A}(k) \ . \ \forall s : k \hookrightarrow K \ . \ S \in \mathrm{Homm}_\sigma(k(a), K) \ .$
$. \ \exists b \in \texttt{Root}(K, \mathrm{minimal}(k)(a)) : S = s_b$

$\texttt{SimpleEmbeddingExtensionSize} :: \forall k, K : \texttt{Field} \ . \ \forall a \in \mathcal{A}(k) \ . \ \forall s : k \hookrightarrow K \ .$
$. \ \#\mathrm{Homm}_s(k(a), K) = \#\texttt{Root}(K, \mathrm{minimal}(k)(a))$

$\texttt{AlgebraicEmbeddingEx} :: \forall k : \texttt{Field} \ . \ \forall K : \texttt{AlgebraicalyClosed} \ . \ \forall L : \texttt{Algebraic}(k) \ .$
$. \ \forall s : k \hookrightarrow K \ . \ \exists S \in \mathrm{Homm}_s(L, K)$

$\texttt{AlgebraicEmbeddingExSpec} :: \forall k : \texttt{Field} \ . \ \forall K : \texttt{AlgebraicalyClosed} \ . \ \forall L : \texttt{Algebraic}(k) \ .$
$. \ \forall s : k \hookrightarrow K \ . \ \forall a \in L \ . \ \forall b \in \texttt{Root}(L, \mathrm{minimal}(k)(a)) \ . \ \exists S \in \mathrm{Homm}_s(L, K) : S(a) = b$

$\texttt{AlgebraicClosuresAreIso} :: \forall k : \texttt{Field} \ .$
$\forall A, B : \texttt{Algebraic}(k) \ \& \ \texttt{AlgebraicalyClosed} \ . \ A \cong_{\mathsf{ALG}(k)} B$

$\texttt{Character} := \prod M : \texttt{Monoid} \ . \ \prod k : \texttt{Field} \ . \ \mathcal{M}_{\mathsf{MON}}(M, K_*,)$

$\texttt{CharacterIndependance} :: \forall T : \texttt{Set Character}(M, k) \ . \ T : \texttt{LinearlyIndependant}(k)$

3.7 Splitting Fields and Normal Extension[?]

$\texttt{SplittinfFieldUnique} :: \forall k : \texttt{Field} \; . \; \forall P : \texttt{Set}\, k[\mathbb{Z}_+] \; . \; \exists! \texttt{SplittingField}(k, P)$

$\texttt{NormalExtensnsionProperty} :: \forall K : \texttt{NormalExtension} \,\&\, \texttt{Algebraic}(k) \; .$
$. \; (\forall s : K \hookrightarrow \overline{k} \; . \; K : \texttt{Invariant}(s)) \,\&\, (\forall p : \texttt{Irreducible}(k) : \exists a \in \texttt{Root}(K, p) \; . \; p : \texttt{Splits}(k))$

$\texttt{NormalClosure} :: \prod k : \texttt{Field}\ \texttt{Algebraic}(k) \to \texttt{NormalExtension}(k)$
$\texttt{NormalClosure}(K) = \mathrm{nc}(K/k) := \min\{L : \texttt{NormalExtension} \,\&\, \texttt{Algebraic}(k) : K \subset L\}$

3.8 Constructable objects[!]

4 Separability