Rings.Know

Uncultured Tramp

September 10, 2016

Contents

1 Basic Rings

1.1 Rings

1.2 Ideals

1.3 Morphisms

1.4 Quotients

1.5 Polynomials and generating functions

$$\texttt{Polynomial} : \texttt{CommutativeRing} \to \texttt{CommutativeRing}$$
$$\texttt{Polynomial}((R) = R[x] := ($$
$$\{p : \mathbb{Z}_+ \to R : \exists N \in \mathbb{Z}_+ : \forall n \in \mathbb{Z}_+ : n \geq N \ . \ p_n = 0\},$$
$$p + q := \Lambda n \in \mathbb{Z}_+ \ . \ p_n + q_n,$$
$$pq := \Lambda n \in \mathbb{Z}_+ \ . \ \sum_{i \in \mathbb{Z}_+} \sum_{j \in \mathbb{Z}_+ : i+j=n} p_i q_j)$$

$$\texttt{degree} :: R[x] \to \mathbb{Z}_+ | - \infty$$
$$\texttt{degree}(p) = \deg p := \texttt{if } p = 0 \texttt{ then } - \infty \texttt{ else } \max\{n \in \mathbb{Z}_+ : p_n \neq 0\}$$

$$\texttt{leadingCoeficient} :: R[x] \to R$$
$$\texttt{leadingCoeficient}(p) = \operatorname{lc}(p) := \texttt{if } p = 0 \texttt{ then } 0 \texttt{ else } p_{\deg p}$$

$$\texttt{Monic} ::?R[x]$$
$$p : \texttt{Monic} \iff \operatorname{lc}(p) = 1$$

$$\texttt{moprhPolyExtension} :: \mathcal{M}_{\mathsf{Ring}}(R, S) \to \mathcal{M}_{\mathsf{Ring}}(R[x], S[x])$$
$$\texttt{moprhPolyExtension}(\phi)(p) = p^{\phi} = \sum_{i=0}^{\infty} \phi(p_i) x^i$$

$$\texttt{Irreducable} ::?R[x]$$
$$f : \texttt{Irreducable} \iff f \, ! \, \texttt{Unit}([R(x)]) \ \& \ \forall p, q \in R[x] : pq = f \ . \ p : \texttt{Unit}([R(x)]) | q : \texttt{Unit}([R(x)])$$

1.5.1 Content and proimitive polinomials

Assume $R : \texttt{UFD}$

$$\texttt{Content} : R[x] \to ?R$$
$$r : \texttt{Content}(p) \iff r \in C(p) \iff r : \texttt{GCD}(\{p_i : i \in \deg p\})$$

$$\texttt{Primitive} :?R[x]$$
$$p : \texttt{Primitive} \iff C(p) = \{1\}$$

$$\texttt{Content} : \mathrm{Frac}\, R[x] \to ?\mathrm{Frac}\, R$$

$$\texttt{Content}(f) = C(f) := \{u\Pi | u : \texttt{Units}(R)\}$$
$$\texttt{Where}$$
$$\Pi = \prod_{P:\texttt{Prime}(R)} P^{e(P)}$$
$$e(P) = \min_{i \in \deg f} \{\exp(f_i, P)\}$$

$$\texttt{Primitive} :: ?\mathrm{Frac} R[x]$$
$$p : \texttt{Primitive} \iff 1 \in C(p)$$

ContentFact1 :: $\forall f \in \mathrm{Frac}\, R \, . \, \forall a \in C(f) \, . \, \exists p \in \texttt{Primitive}(R) : f = ap$
Proof $\approx$
Let $a = u\Pi$ as in definition of content. Then, by definition of Π

$$(u\Pi)^{-1} f = \sum_{i=0}^{\deg f} r_i x^i = p$$

with each $r_i \in R$ such that $gcd(r) = 1$ which means that p is Primitive and in $R[x]\square$.

ContentFact2 :: $\forall p : \texttt{Primitive}(\mathrm{Frac}\, R) \, . \, p : \texttt{Primitive}(\mathrm{Frac}\, R)$
Proof $\approx$
We know that $1 \in (p)$ so by ContentFact1 $p = 1p$ lies in $R[x]$.

ContentFact3 :: $f \in R[x] \iff C(f) \in R$
Proof $\approx$
If $f \in R[x]$ when all her coefficients lie in R so by definition of content in field of fractions $C(f) \in R$.
If $C(f) \in R$ when by definition of C no prime factor of any coefficient of f has strictly negative exponent which is the same as $f \in R[x]$.

GausLemma :: $\forall f, g : \texttt{Primitive}(R) \, . \, fg : \texttt{Primitive}(R)$
Proof $\approx$
Assume f, g are primitive polynomials.
Assume fg Is not primitive.
This means that there exists a prime element $p \in R$ such that $p \in C(fg)$.
Let $\pi_p : R \to \frac{R}{(p)}$ denote natural projection.
Then

$$0 = (fg)^{\pi_p} = f^{\pi_p} g^{\pi_p}$$

but as f and g are primitive $f^{\pi_p} g^{\pi_p} \neq 0$ so we have a contradiction.
$\square$

ContentProduct $:: \forall f, g : \operatorname{Frac} R[x] \,.\, C(fg) = C(f)C(g)$
Proof $\approx$
For each $a \in C(f)$ and $b \in C(g)$ by ContentFact1 we write $f = aF$ and $g = aG$ whera F and G are primitive and hence by GausLemma FG is primitive.
So

$$C(fg) = C(aFbG) = C(abFG) = ab\texttt{Unit}(R) = a\texttt{Unit}(R)b\texttt{Unit}(R) = C(f)C(g)$$

□
PrimitiveFactorization $:: \forall f \in R[x] \,.\, \forall h \in \operatorname{Frac} R[x] \,.\, \forall p : \texttt{Primitive}(R) : f = ph \,.\, h \in R[x]$
Proof $\approx$ By ContentProduct and using permittivity of p we have

$$C(f) = C(ph) = C(p)C(h) = C(h)$$

so by contentFact3 $h \in R[x]$.
□

1.5.2 Irreducibility over field of fractions

FactorizationOver $: R[x] \to ?R \to ?(R[x] \times R[x])$
$(a, b) : \texttt{FactorizationOver}(f)(S) \iff f = ab \wedge \forall i \in \deg a \,.\, a_i \in S \wedge \forall i \in \deg b \,.\, b_i \in S$

DegreewiseFactorization $: R[x] \to ?R \to ?(R[x] \times R[x])$
$(a, b) : \texttt{DegreewiseFactorization}(f) \iff f = ab \wedge \deg a > 0 \wedge \deg b > 0$

DegreewiseIrrefucable $:?R[x]$
$f : \texttt{DegreewiseIrreducable} \iff \forall (a, b) \in R[x] \times R[x] \,.\, (a, b) \,!\, \texttt{DegreewiseFactorization}(f)$

IrreducibilityInFractionsTheorem1 $:: \forall f \in R[x] \,.\, f : \texttt{DegreewiseIrreducable}(R) \iff f : \texttt{DegreewiseIrreducable}(\operatorname{Frac} R)$
Proof $\approx$
One side is trivial .
Now assume that f is degreewise irreducible only in R. Assume that (a, b) is a degreewise factorisation of f in field of fractions. let α be an element from content of a such that $a = \alpha p$ where p is primitive. Then

$$f = ab = \alpha pb = (\alpha b)p.$$

As $f \in R[x]$ and p is primitive then by PrimitiveFactorization $(\alpha b) \in R[x]$ and by ContentFact2 $p \in R[x]$. So f is not irreducible over R, a contradiction.
□

IrreducibilityInFractionsTheorem1 $:: \forall f : \texttt{Primitive}\, R[x] \,.\, f : \texttt{eIrreducable}(R) \iff f : \texttt{Irreducable}(\operatorname{Frac} R)$
Proof $\approx$
If f is not irreducible only in R then one of her factors must have a degree 0 which means that f is not primitive.
A contradiction.
If f is not irreducible only in field of fractions then it must be degreewise reducible and hence reducible in R also.
A contradiction. □

1.5.3 Division Algorithm

`DivisionAlgorithm` $:: \forall f \in R[x] . \forall g : \texttt{Monic}(R) \; . \; \exists q, r \in R[x] : \deg r \leq \deg g : f = gq + r$

`Proof` $\approx$

If $\deg g > \deg f$ then just take $q = 0$ and $r = f$.

Otherwise we know that $\deg q = \deg f - \deg g$ so we can choose q_i to be unique to be unique solution of linear equation $((gq)_i = f_i)_{i=\deg g}^{\deg f}$ which always exists as g is monic and $(R, +)$ is a group.

So $\deg r \leq \deg f$. $\square$.

`RootIsFactor` $:: \forall f \in R[x] \; . \; \forall a \in R \; . \; a : \texttt{Root}(f) \iff x - a : \texttt{Factor}(f)$

`Proof` $\approx$

Represent $f = q(x - a) + r$.

If a is root of f then $0 = f(a) = q(a - a) + r = r$, so $(x - a)$ is indeed a factor of f.

Another side is trivial $f(a) = q(a - a) = 0$. $\square$.

`MaximalRoots` $:: \forall f \in R[x] \; . \; \# \ker f \leq \deg f$

`Proof` $\approx$ number of factors of a polynomial cannot exceed her degree and number of roots cannot exceed her degree.

2 Characteristic

3 Classes of Commutative rings

3.1 Integral Domains

3.2 Unique Factorization Domain

3.3 PID

3.4 Euclidean Domains