Abstract algebra: Homework 9

Northwestern Polytechnic University

Due on Monday, Dec. 10^{th}

2.3 Principal ideal domains

Exercise 2.3.2 (3P). Let $(S, \cdot)$ be an abelian monoid (commutative semi-group with neutral element id) that is cancellative, i.e. for every $a, b, c \in S$, $ab = ac$ implies $b = c$. Construct a group of fractions $K[S]$ and state and show its universal property.
Hint: The universal property should consider maps into any abelian group $(A, \cdot)$.

Extra Exercise 2.3.3 (5XP). Given a non-commutative (unital) integral ring R (i.e. an associative $\mathbb{Z}$-algebra with $ab = 0$ implies $a = 0$ or $b = 0$) that fulfills the Ore condition: Every finite intersection of non-trivial principal ideals is nontrivial. Show that the analogon of the field construction gives a division algebra, i.e. $S[R] := (R \times R \setminus 0)/\sim$ where $a/b \sim c/d$ iff $ad = cb$ (in that order). Show that

0. $\sim$ is an equivalence relation;

a. the addition $a/b + c/d = (af + bg)/p$ for $a, b, c, d \in R$, $c, d \neq 0$ and $p, f, g \in R \setminus 0$ such that $bf = p = dg$ is well-defined and forms an abelian group. Note that you have to show existence of some (p, f, g) as well as $a/b + c/d \sim a'/b' + c'/d'$ for all pairs $a/b \sim a'/b'$ and $c/d \sim c'/d'$. (What is the neutal element, the inverses?)

b. the multiplication $(a/b) * (c/d) = \tilde{a}/\tilde{d}$ for $a, b, c, d \in R$, $b, c, d \neq 0$, and some $\tilde{a}, \tilde{b}, \tilde{d} \in R$ with $\tilde{a}/\tilde{b} \sim a/b$ and $\tilde{b}/\tilde{d} \sim c/d$. Extend by $(a/b) * (0/d) = (0/1)$ and show that multiplication is also well-defined and gives a (non-commutative) ring structure.

c. Show that $S[R]$ is a division-ring generated by $\imath\colon R \to S[R] : a \mapsto a/1$. You can, e.g. show that $(a/b)/(c/d) = \tilde{a}/\tilde{c}$ for $a, b, c, d \in R$ with $b, c, d \neq 0$ and some $\tilde{a}, \tilde{b}, \tilde{c} \in R \setminus 0$ with $a/b \sim \tilde{a}/\tilde{b}$ and $c/d \sim \tilde{c}/\tilde{b}$ is well-defined and gives the inverse elements.

Exercise 2.3.4 (2P). Let R be a ring and $\partial\colon R[x] \to R[x] : R \to 0, x \mapsto 1$ the standard derivative. Show that

a. if $p_1 \in R[x]$ is a polynomial, $p := (x - a)p_1 \in R[x]$ with $a \in R$, then ∂p has root a iff p_1 has root a;

b. conclude that for $p \in F[x]$ where F is a field, then the roots of $\gcd(p, \partial p)$ are exactly the multiple roots of p. (This will be helpful in the section about discriminants of polynomials.)

Exercise 2.3.5 (3P). Let R be a domain and denote $F := K[R]$ the field of fractions of R.

a. Show that $K[R[x]\,] = F(x)$ where x is an indeterminate over R and $F(x)$ is the field of rational functions p/q for $p, q \in F[x]$ and $q \neq 0$.

c. Show that $F(\!(x)\!) := K[R[\![x]\!]\,] = F[[x], x^{-1}]$ where $F[[x], x^{-1}]$ are the formal Laurent series, i.e. the power series starting with a finite integer possibly negative exponent.

Hint: Remember the geometric series, i.e. for $|q| < 1$, $\frac{1}{1-q} = 1 + q + q^2 + \dots$ and use this to invert a formal power series (in terms of power series with finite coefficients).

d. Show that the embedding $R[x] \to R[[x]]$ induces an embedding $F(x) \to F(\!(x)\!)$ that maps a rational function to a Laurent series. What element is $1/(1 + x + x^2) \in F(x)$ mapped to?

Exercise 2.3.8 (2P). Let $(R[x], \partial)$ be a differential ring and R be an integral domain. Show that ∂ extends uniquely to $K[R[x]\,] = F(x)$ with $F = K[R]$ and $F(x)$ as in Exercise 2.3.5a. Express the constants $\mathrm{Const}(F(x))$ in terms of $\mathrm{Const}(R[x])$.
Hint: Show the quotient rule using the product/Leibniz rule.

2.4 Unique Factorization Domains

Exercise 2.4.1 (2P). Compute the gcd and lcm of $x^2 + x - 1$, $x^3 + x - 1$, and $x^4 + x^2 - 1$ over $\mathbb{Q}$.

Exercise 2.4.2 (1P). Show that no poynomial ring in more than one indeterminate is a PID.

Exercise 2.4.4 (2P). Show that for every family $(a_i)_{i\in I}$ of elements $a_i \in R$ of a PID the greatest common divisor can be written as finite linear combination $\gcd = \sum_{j=1}^{n} c_j a_{i_j}$ for some $i_j \in I$, $n \in \mathbb{N}$ and $c_j \in R$.

Exercise 2.4.6 (3P). Write down all irreducible polynomials in $\mathbb{F}_2[x]$ of degree 5.

Exercise 2.4.8 (2P). Write in partial fractions

$$\frac{x^5+1}{x^4+x^2} \in \mathbb{F}_2(x), \tag{a}$$

$$\frac{x^5+1}{x^4+x^2} \in \mathbb{F}_3(x), \tag{b}$$