# MATH 7210 Homework 7

Andrea Bourque

October 2021

## 1 Problem 1

Let $R((X))$ be the ring of formal Laurent series over the commutative ring $R$ with 1. Let $R[[X]]$ be the subring of formal power series.

a) Show that $R[[X]]^\times = \{a_0 + a_1X + ... \mid a_0 \in R^\times\}$.

*Proof.* Let $a_0 + a_1X + ... \in R[[X]]^\times$, and let $b_0 + b_1X + ...$ be its inverse. Then $1 = (a_0 + a_1X + ...)(b_0 + b_1X + ...) = a_0b_0 + (a_0b_1 + a_1b_0)X + ...$, implying that $a_0b_0 = 1$. Thus $a_0 \in R^\times$.

Now let $a_0 \in R^\times$ and let $a_0 + a_1X + ... \in R[[X]]$. Let $b_0 = a_0^{-1}$. Now assume that we have coefficients $b_0, ..., b_n$ such that $(a_0+a_1X+...)(b_0+b_1X+...b_nX^n) = 1+O(X^{n+1})$. The coefficient of $X^{n+1}$ in $(a_0+a_1X+...)(b_0+b_1X+...+b_{n+1}X^{n+1})$ is $a_0b_{n+1} + a_1b_n + ... + a_{n+1}b_0$. For this to be 0, we have $b_{n+1} = -a_0^{-1}(a_1b_n + ... + a_{n+1}b_0)$. Therefore, by induction, we have an inverse to $a_0 + a_1X + ...$ given by $b_0 + b_1X + ....$ □

b) If $R$ is an integral domain, what is $R((X))^\times$?

*Proof.* A nonzero element in $R((X))$ is uniquely expressed as $X^{n_0}(a_0+a_1X+...)$ for $n_0 \in \mathbb{Z}$ and $a_0 \neq 0$. Consider some other nonzero element $X^{m_0}(b_0+b_1X+...)$. Their product is $X^{n_0+m_0}(a_0b_0 + (a_0b_1 + a_1b_0)X + ...)$. Since $a_0, b_0 \neq 0$ and $R$ is an integral domain, $a_0b_0 \neq 0$, so $X^{n_0+m_0}(a_0b_0 + (a_0b_1 + a_1b_0)X + ...)$ has a lowest degree term of $X^{n_0+m_0}$. Thus, if the product is to be 1, we must have $n_0 + m_0 = 0$ and $a_0b_0 = 1$. Thus $R((X))^\times$ consists of $X^{n_0}(a_0 + a_1X + ...)$ with $a_0 \in R^\times$. □

c) Show that if $R$ is an integral domain, so are $R[[X]]$ and $R((X))$.

*Proof.* Since $R[[X]]$ is a subring of $R((X))$, it suffices to show that $R((X))$ is an integral domain. To that end, let $X^{n_0}(a_0 + a_1X + ...)$ and $X^{m_0}(b_0 + b_1X + ...)$ be nonzero elements in $R((X))$; that is, $a_0, b_0 \neq 0$. The product is $X^{n_0+m_0}(a_0b_0+(a_0b_1+a_1b_0)X+...)$. Since $R$ is an integral domain, $a_0b_0 \neq 0$, so $X^{n_0+m_0}(a_0b_0+(a_0b_1+a_1b_0)X+...) \neq 0$. Thus $R((X))$ is an integral domain. □

d) If $F$ is a field, show that $F((X))$ is the fraction field of $F[[X]]$.

*Proof.* Since a field is an integral domain, we have that $F((X))^\times$ consists of $X^{n_0}(a_0 + a_1X + ...)$ with $a_0 \in F^\times$ by part b. But $F^\times = F - \{0\}$, so all nonzero elements of $F((X))$ are invertible. Thus $F((X))$ itself is a field, containing $F[[X]]$ as a subring. By part c, we have $F[[X]]$ is an integral domain. By Corollary 7.5.16 in Dummit and Foote, the fraction field of $F[[X]]$ is then the subfield of $F((X))$ generated by $F[[X]]$. But $F((X))$ is generated by $F[[X]]$, since the nonzero elements are $X^{n_0}(a_0+a_1X+...)$, where $a_0+a_1X+... \in F[[X]]$, and $X^{n_0}$ or $(X^{n_0})^{-1} = X^{-n_0}$ are in $F[[X]]$. Thus $F((X))$ is the fraction field of $F[[X]]$. □

e) Show that the fraction field of $\mathbb{Z}[[X]]$ is a proper subfield of $\mathbb{Q}((X))$.

*Proof.* We again have that $\mathbb{Z}[[X]]$ is an integral domain contained in the field $\mathbb{Q}((X))$, so by Corollary 7.5.16 in Dummit and Foote, the fraction field of $\mathbb{Z}[[X]]$ is a subfield of $\mathbb{Q}((X))$. It suffices to find an element of $\mathbb{Q}((X))$ which is not contained in the fraction field of $\mathbb{Z}[[X]]$. Enumerate the prime numbers as $p_1, p_2, ....$ Then consider $f(X) = 1 + \frac{1}{p_1}X + \frac{1}{p_2}X^2 + ...$ . Suppose $a_0 + a_1X + ... \in Z[[X]]$ and $(a_0 + a_1X + ...)f \in Z[[X]]$. Then for all $n$, $\frac{a_0}{p_n} + ... + a_n \in \mathbb{Z}$. In the sum, the only time the prime $p_n$ occurs in a denominator is in $\frac{a_0}{p_n}$. Then, in order for this to be an integer, $p_n$ must divide $a_0$. Since this hold for all primes $p_n$, we must have that $a_0 = 0$. Then we must have $(a_1 + a_2X + ...)f \in \mathbb{Z}[[X]]$. Inductively, we can show that $a_n = 0$ for all $n$, so $(a_0 + a_1X + ...)f = 0$. Therefore, $f$ cannot be in the fraction field of $\mathbb{Z}[[X]]$, since it is nonzero, yet $\mathbb{Z}[[X]]f \cap \mathbb{Z}[[X]] = \{0\}$. □

## 2 Problem 2

Let $R$ be commutative with 1, and let $f(X) \in R[X]$ be monic of degree $n \geq 1$. Let $S = R[X]/(f(X))$. $\overline{p(X)}$ denotes the coset of $p(X)$ in $S$.

a) Show that every element of $S$ is of the form $\overline{p}$ for some polynomial $p$ of degree less than $n$.

*Proof.* Let $f(X) = a_0 + a_1X + ...X^n$. Let $\overline{q} \in S$ with $q = b_0 + ...b_mX^m$, where $m \geq n$. Since we are quotienting by $(f(X))$, we can inductively reduce $q$ by taking $q_1 = q - b_mX^{m-n}f$, which is in the same coset as $q$, and furthermore has degree less than $m$. By repeating this process, we gain a representative $p$ for $\overline{q} \in S$. □

b) Show that the above representation is unique.

*Proof.* If $p, q$ are representatives for the same coset in $S$, both having degree less than $n$, we must have $f|(p-q)$. But the degree of $p-q$ is less than $n$, which is a contradiction, unless $p = q$. □

c) If $f = pq$ with $p, q$ of degree less than $n$, show that $\overline{p}$ is a zero divisor in $S$.

*Proof.* We have $(\overline{p})(\overline{q}) = \overline{pq} = \overline{f} = \overline{0}$. If $\overline{p} = \overline{0}$, that would imply $f|p$, which is impossible by degree. Further, $p \neq 0$ since that would imply $f = 0$. Similarly, $\overline{q} \neq \overline{0}$. Thus we have two nonzero elements in $S$ multiplying to the 0 element. □

# 3 Problem 3

a) Show that $S = (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$ has 4 elements.

*Proof.* By the results of problem 2, each element of $S$ has a unique representative by a polynomial with degree less than 2. There are 4 such polynomials: $0, 1, X, X + 1$. □

b) Show that $(S, +)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

*Proof.* An explicit isomorphism is given by $\overline{a_0 + a_1 X} \mapsto (a_0, a_1)$. In particular, $\overline{1}$ and $\overline{X}$ generate $S$: $\overline{1} + \overline{1} = \overline{0}$, $\overline{X} + \overline{X} = \overline{0}$, and $\overline{X} + \overline{1} = \overline{X + 1}$. □

c) Show that $(S - \{\overline{0}\}, \cdot)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Conclude that $S$ is a field with 4 elements.

*Proof.* An explicit isomorphism is given by $\overline{1} \mapsto 0, \overline{X} \mapsto 1, \overline{X + 1} \mapsto 2$. In particular, $\overline{X}$ generates $S - \{0\}$: $X^2 = (X^2 + X + 1) + X + 1$, so $\overline{X}^2 = \overline{X + 1}$. $\overline{X}^3 = \overline{X(X + 1)} = \overline{X^2 + X} = \overline{X^2 + X + 1 + 1}$, so $\overline{X}^3 = \overline{1}$. Since each non-zero element of $S$ is invertible ($\overline{X(X + 1)} = \overline{1}$), $S$ is a field. □

# 4 Problem 7.3.15

Let $X$ be a nonempty set and let $\mathcal{P}(X)$ be the Boolean ring on the power set, with addition by symmetric difference and multiplication by intersection. Let $R$ be the ring of all functions from $X$ to $\mathbb{Z}/2\mathbb{Z}$. For each $A \in \mathcal{P}(X)$ define the function $\chi_A : X \to \mathbb{Z}/2\mathbb{Z}$ by $\chi_A(x) = 1$ if $x \in A$ and $\chi_A(x) = 0$ if $x \notin A$. Prove that $\psi : \mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring isomorphism.

*Proof.* Recall that the additive identity in $\mathcal{P}(X)$ is $\emptyset$, and the multiplicative identity is $X$. Furthermore, the multiplicative identity in $R$ is the constant function $1(x)$, and the additive identity is the constant function $0(x)$.

First we show that $\psi$ is a ring homomorphism. $\psi(X) = \chi_X$, and $\chi_X(x) = 1$ for all $x \in X$ by definition, since $x \in X$. Thus $\chi_X(x) = 1(x)$.

Next, let $C = A + B = (A - B) \cup (B - A)$. $\psi(C) = \chi_C$ satisfies $\chi_C(x) = 1$ if $x \in C$. Then $x \in A - B$ or $x \in B - A$. If $x \in A - B$, then $\chi_A(x) = 1$ and $\chi_B(x) = 0$, so $\chi_C(x) = 1 = 1+0 = \chi_A(x)+\chi_B(x)$. Similarly, if $x \in B-A$, then $\chi_C(x) = 1 = 0+1 = \chi_A(x)+\chi_B(x)$. If $x \notin C$, then $x \in A \cap B$ or $x \notin A \cup B$. If $x \in A \cap B$, then $\chi_A(x) = \chi_B(x) = 1$, and $\chi_C(x) = 0 = 1 + 1 = \chi_A(x) + \chi_B(x)$. If $x \notin A \cup B$, then $\chi_A(x) = \chi_B(x) = 0$, and $\chi_C(x) = 0 = 0+0 = \chi_A(x)+\chi_B(x)$. In all possible cases, we have $\chi_C(x) = \chi_A(x)+\chi_B(x)$, showing that $\psi(A+B) = \psi(A) + \psi(B)$.

Let $C = A \cdot B = A \cap B$. Then $\chi_C(x) = 1$ if $x \in A \cap B$ and $\psi_C(x) = 0$ if $x \notin A \cap B$; $x \notin A$ or $x \notin B$. If $x \in A \cap B$, then $\chi_A(x) = \chi_B(x) = 1$, and $\chi_C(x) = 1 = 1 \cdot 1 = \chi_A(x)\chi_B(x)$. If $x \notin A \cap B$, then one of $\chi_A(x)$ and $\chi_B(x)$ is 0, implying their product is 0. Then $\chi_C(x) = 0 = \chi_A(x)\chi_B(x)$. In any case, $\psi(A \cdot B) = \psi(A)\psi(B)$.

Now we show $\psi$ is an isomorphism. If $\psi(A) = 0(x)$, then $\chi_A(x) = 0$ for all $x \in X$, implying $x \notin A$ for all $x \in X$. As $A \subset X$, this implies $A = \emptyset$, so $\psi$ has 0 kernel. This means $\psi$ is injective.

Now let $f : X \to \mathbb{Z}/2\mathbb{Z}$. Let $A = f^{-1}(\{1\})$. Then $\chi_A(x) = 1$ if $x \in A$, i.e. if $f(x) = 1$, and $\chi_A(x) = 0$ if $x \notin A$, i.e. if $f(x) \neq 1$. But $f(x) \neq 1$ implies $f(x) = 0$. Thus $\chi_A = f$, implying that $\psi(A) = f$, so $\psi$ is surjective. Thus $\psi$ is a ring isomorphism. □

# 5 Problem 7.5.3

Let $F$ be a field. Prove that $F$ contains a unique smallest subfield $F_0$ and that $F_0$ is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$.

*Proof.* Consider the subfield $F_0$ generated by 0 and 1. Since any subfield of $F$ contains 0 and 1, they must necessarily contain $F_0$. It follows then that $F_0$ is the unique smallest subfield of $F$.

Now consider a homomorphism $f : \mathbb{Z} \to F$. Since $f(0) = 0, f(1) = 1$, $f(\mathbb{Z}) \subset F_0$. Now, if $\ker f = 0$, then $\mathbb{Z} \cong f(\mathbb{Z})$, and so $F_0$ contains the fraction field of $f(\mathbb{Z})$, which is isomorphic to $\mathbb{Q}$. But $F_0$ is the smallest subfield of $F$, implying $F_0 \cong \mathbb{Q}$.

If $\ker f \neq 0$, then $\ker f = (n)$ for some integer $n$. $\ker f \neq \mathbb{Z}$ since $f(0) = 0 \neq 1 = f(1)$. Assume $n = mk$ with $m, k < n$. Then $f(m)f(k) = f(mk) = f(n) = 0$. But $f(m), f(k) \neq 0$ since $m, k \notin (n)$. Thus $f(m)$ is a zero divisor in $F$, which is impossible. It follows that $n$ must be prime, say $n = p$. Then $F_0$ contains $f(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, which is a field. Since $F_0$ is the smallest subfield of $F$, $F \cong \mathbb{Z}/p\mathbb{Z}$. □