Math 323 Homework 3

Problem 2 (Chapter 2.9)

Show that if D is a domain and F_1 and F_2 are fields such that D is a subring of each and each is generated by D, then there is a unique isomorphism of F_1 onto F_2 that is the identity map on D.

Solution. ff Use the universal property.

Theorem 2.9: Let D be a commutative domain, F its field of fractions. Then any monomorphism η_D of D into a field F' has a unique extension to a monomorphism of η_F of F into F'.

Since D is a subring of F_1 and F_2, we have the natural embedding of D in F_1, $\eta_1 \colon D \hookrightarrow F_1$, and the natural embedding of D in F_2, $\eta_2 \colon D \hookrightarrow F_2$. Since η_1, η_2 are injective, their inverses are

Some Oakley wisdom: when we say the fields such that $\{\text{Fields } F \supset D\}$, we can't say a smallest field because there is no order on all fields. But if we consider subfields of F_1, $S = \{K \colon F_1 \supset K \supset D\}$, then saying F_1 is the smallest is like saying $S = \{F_1\}$.

So we have the commutative diagram, $D \to F, D \to K(D), K(D) \to F$ (last arrow unique). But we must have that $K(D) = F_1$, so F_1 is isomorphic to the field of fractions. Both of them are, so we are done.

Also to use theorem, we need D commutative. But since D is in a field, we have $a, b \in D$, and so in F, $ab = ba$, but in D.

Problem 5 (Chapter 2.9)

Let R be a commutative ring, and S a submonoid of the multiplicative monoid of R. In $R \times S$ define $(a, s) \sim (b, t)$ if there exists a $u \in S$ such that $u(at - bs) = 0$. Show that this is an equivalence relation in $R \times S$. Denote the equivalence class of (a, s) as a/s and the quotient set consisting of these classes as RS^{-1}. Show that RS^{-1} becomes a ring relative to

$$\begin{aligned} a/s + b/t &= (at + bs)/st \\ (a/s)(b/t) &= ab/st \\ 0 &= 0/1 \\ 1 &= 1/1 \end{aligned}$$

Show that $a \to a/1$ is a homomorphism of R into RS^{-1} and that this is a monomorphism if and only if no element of S is a zero divisor in R. Show that the elements $s/1$, $s \in S$, are units in RS^{-1}.

Solution. ff

Problem 2 (Chapter 2.10)

Show that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and that the real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$. Show that $u = \sqrt{2} + \sqrt{3}$ is algebraic and determine an ideal I such that $\mathbb{Q}[x]/I \cong \mathbb{Q}[u]$.

Solution. Assume there exists $a_0, a_1, \dots \in \mathbb{Q}$ such that $\sqrt{3} = a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + a_3(\sqrt{2})^3 + \cdots$, which clearly is equivalent to there being $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$ (since each term is either an element in $\mathbb{Q}$, or an element in $\mathbb{Q}$ times $\sqrt{2}$). If we square both sides, we get $3 = a^2 + 2b^2 + 2ab\sqrt{2} \implies \sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$ (since $\mathbb{Q}$ is a field), but by any standard proof, $\sqrt{2} \notin \mathbb{Q}$, a contradiction. Hence, there do not exist $a, b \in \mathbb{Q}$, and so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

Recall from linear algebra it is sufficient to show, when $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, that $a_0(1) + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} = 0$ only when $a_0 = a_1 = a_2 = a_3 = 0$. ff

We want to show that there exists an $n \in \mathbb{N}^0$ and nonzero $a_i \in \mathbb{Q}$ such that $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$. We have

$$1 - 10u^2 + u^4 = 1 - 50 - 20\sqrt{6} + 49 + 20\sqrt{6} = 0$$

Hence, $u = \sqrt{2} + \sqrt{3}$ is algebraic.

We want to find I such that $u = x + I$. I'm pretty sure this is $1 - 10x^2 + x^4$. ff

Problem 4 (Chapter 2.10)

Let $\Delta = \prod_{i>j}(x_i - x_j)$ in $\mathbb{Z}[x_1, \dots, x_r]$ and let $\zeta(\pi)$ be the automorphism of $\mathbb{Z}[x_1, \dots, x_r]$ which maps $x_i \to x_{\pi(i)}, 1 \leq i \leq r$. (Every automorphism of the ring $\mathbb{Z}[x_1, \dots, x_r]$ is the identity on $\mathbb{Z}$. Why?) Verify that if τ is a transposition then $\Delta \to -\Delta$ under $\zeta(\tau)$. Use this to prove the result given in section 1.6 that if π is a product of an even number of transpositions, then every factorization of π as a product of transpositions contains an even number of transpositiitions. Show that $\Delta^2 \to \Delta^2$ under every $\zeta(\pi)$.

Solution. First, note that every automorphism of $\mathbb{Z}[x_1, \dots, x_r]$ is the identity on $\mathbb{Z}$, since ff

Let $\tau = (mn)$ be a transposition, where $1 \leq m, n \leq r$, $m \neq n$. Without loss of generality, let $n > m$. Since ζ is an automorphism, we have $\zeta(\tau)(\Delta) = \prod_{i>j} \zeta(\tau)(x_i - x_j) = \prod_{i>j}(x_{\tau(i)} - x_{\tau(j)})$. Consider each factor, $(x_{\tau(i)} - x_{\tau(j)})$. If $\tau(i) = i$ and $\tau(j) = j$, then $(x_{\tau(i)} - x_{\tau(j)}) = (x_i - x_j)$. If $\tau(i) = k$ and $\tau(j) = j$, we have that $(x_{\tau(i)} - x_{\tau(j)}) = (x_j - x_k)$, but we must have then $\tau(k) = i$ and there is some other factor $(x_{\tau(j)} - x_{\tau(k)}) = (x_j - x_i)$, and multiplication of polynomials is commutative, so we can swap these two terms and nothing changes. If $\tau(i) = j$ so $\tau(j) = i$, we have $(x_{\tau(j)} - x_{\tau(j)}) = (x_i - x_j) = -(x_j - x_i)$. This covers all the possible case in the product of Δ, and so, since there is only one factor that changes, specifically by picking up a negative, we have $\zeta(\tau)(\Delta) = -\Delta$.

The result from 1.6 then follows, since ff (negative sign)

Recall that every π can be decomposed as a product of transpositions. Hence, if $\pi = \tau_n \circ \tau_{n-1} \circ \cdots \circ \tau_1$, we have $\zeta(\pi) = \zeta(\tau_n) \circ \zeta(\tau_{n-1}) \circ \cdots \circ \zeta(\tau_1)$. Since $\zeta(\pi)$ is an automorphism, we have $\zeta(\pi)(\Delta^2) = (\zeta(\pi)(\Delta))^2$. So

$$\zeta(\pi)(\Delta^2) = ((\zeta(\tau_n) \circ \zeta(\tau_{n-1}) \circ \cdots \zeta(\tau_1))(\Delta))^2 = (\pm\Delta)^2 = \Delta$$

where the second to last equality is from the fact $\zeta(\tau)(\Delta) = -\Delta$.

Problem 7 (Chapter 2.10)

Let $R[[x]]$ denote the set of unrestricted sequences $(a_0, a_1, \dots)$, $a_i \in R$. Show that one gets a ring from $R[[x]$ if one defines $+, \cdot, 0, 1$ as in the polynomial ring. This is called the ring of formal power series in one indeterminate.

Solution. ff just copy book

Problem 1 (Chapter 2.11)

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in F$, a field, $n > 0$ and let $u = x + (f(x))$ in $F[x]/(f(x))$. Show that every element of $F[u]$ can be written in one and only one way in the form $b_0 + b_1 u + \cdots + b_{n-1} u^{n-1}$, $b_j \in F$.

Solution. ff

Problem 2 (Chapter 2.11)

Take $F = \mathbb{Q}$, $f(x) = x^3 + 3x - 2$ in exercise 1. Show that $F[u]$ is a field and express the elements

$$(2u^2 + u - 3)(3u^2 - 4u + 1), \qquad (u^2 - u + 4)^{-1}$$

as polynomials of degree ≤ 2 in u.

Solution. ff

Problem 3 (Chapter 2.11)

(a). Show that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorhpic.

(b). Let $\mathbb{F}_p = \mathbb{Z}/(p)$, p a prime, and let $R_1 = \mathbb{F}_p[x]/(x^2 - 2)$, $R_2 = \mathbb{F}_p[x]/(x^2 - 3)$. Determine whether $R_1 \cong R_2$ in each of the cases in which $p = 2$, 5, or 11.

(a). *Solution.* ff

(b). *Solution.* ff

Problem 4 (Chapter 2.11)

Show that x^3+x^2+1 is irreducible in $(\mathbb{Z}/(2))[x]$ and that $(\mathbb{Z}/(2))[x]/(x^3+x^2+1)$ is a field with eight elements.

Solution. Recall $I_1+I_2 := (I_1 \cup I_2)$. If $a_1 \in I_1$ and $a_2 \in I_2$, then $a = 0$ works. If $a_1 \in I_1$ but $a_2 \notin I_2$ (and so $a_2 \in I_1$ since $a_2 = i_1 + i_2$ and ff hmm now this seems a lot more trivial, we have $a = a_2$ works, since $a_1 - a_2 \in I_1$ since I is a subgroup with respect to addition, and $a_2 - a_2 = 0 \in I_2$ since I_2 must contain the zero since it is a group with respect to addition. The same works when $a_1 \notin I_1$ and $a_2 \in I_2$, i.e. $a = a_1$. ff