Submit problems 3, 9, 10 by Thursday, August 17. Concepts covered: Irreducible polynomials, Field extensions, Characteristic of a field. Reading: Rotman section on Prime and Maximal ideals.

1. Let R be an integral domain then associated to it is a field called its field of fractions $Q(R)$. As a set
$$Q(R) = \{(a, b) \in R \times R \mid b \neq 0\} / \sim$$
where $(a, b) \sim (c, d)$ if $ad = bc$. We denote the equivalence classes by $\dfrac{a}{b}$.
   (a) Show that under the operations $a/b + c/d = (ad + bc)/(bd)$ and $(a/b) \cdot (c/d) = (ac)/(bd)$ $Q(R)$ is a field. What are the additive and multiplicative identities?
   (b) Show that the map $\imath : R \to Q(r)$ given by $\imath(a) = a/1$ is an injective ring homomorphism. Hence we can consider R as a subring of $Q(R)$ under this homomorphism.
   (c) Let $\phi : R \to F$ be a ring homomorphism where F is a field then show that ϕ extends to a ring homomorphism $\bar{\phi} : Q(R) \to F$ if and only if ϕ is injective. Infer that $Q(\mathbb{Z}) = \mathbb{Q}$.
   (d) If R is a field what is $Q(R)$.

2. If F is a field we denote $Q(F[x])$ be $F(x)$. This is the field of rational functions in over F in one variable. Describe $F(x)$. If $E \supset F$ is a field extension and $a \in E$, there is a ring homomorphism $\phi_a : F[x] \to E$ given by $\phi_a(p) = p(a)$. When does ϕ_a extend to $F(x)$?

3. Let F be a field and $G \subset F^\times$ a finite multiplicative sub-group of the group of units.
   (a) Show that G can not be isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for any $p \in \mathbb{Z}$ prime.
   (b) (**Bonus**) Show that G is cyclic.

4. Problem 52, page 37 Rotman.

5. Problem 55, page 38 Rotman.

6. Problem 56, Rotman.

7. Problem 57, Rotman.

8. Problem 58, Rotman.

9. Problem 59.

10. Find irreducible polynomials of degree 2 and 3 over $\mathbb{Z}/2\mathbb{Z}[x]$. Construct fields F_4 and F_8 of order 4 and 8 respectively.
   (a) Write down the multiplication table of F_4.
   (b) Show that in F_4 all elements are roots of $x^4 - x$ and in F_8 all elements elements are roots of $x^8 - x$.
   (c) Show that F_4 does not embed in F_8.

We claim that F is a field, which will complete the proof. If $a, b \in F$, then $a^q = a$ and $b^q = b$. Therefore, $(ab)^q = a^q b^q = ab$, and $ab \in F$. By Lemma 32(iii), replacing b by $-b$, we have $(a - b)^q = a^q - b^q = a - b$, so that $a - b \in F$. Finally, if $a \neq 0$, then $a^{q-1} = 1$ so that $a^{-1} = a^{q-2} \in F$ (because F is closed under multiplication). •

In Corollary 53 we shall see that any two fields of order p^n are isomorphic. It will follow that there are no finite fields other than those just constructed.

Exercises

49. A polynomial $p(x) \in F[x]$ of degree 2 or 3 is irreducible over F if and only if F contains no root of $p(x)$. (This is false for degree 4: the polynomial $(x^2 + 1)^2$ factors in $\mathbb{R}[x]$, but it has no real roots.)

50. Let $p(x) \in F[x]$ be irreducible. If $g(x) \in F[x]$ is not constant, then either $(p(x), g(x)) = 1$ or $p(x) \mid g(x)$.

51. (i) Every nonzero polynomial $f(x)$ in $F[x]$ has a factorization of the form

$$f(x) = ap_1(x) \cdots p_t(x),$$

where a is a nonzero constant and the $p_i(x)$ are (not necessarily distinct) monic irreducible polynomials;

(ii) the factors and their multiplicities in this factorization are uniquely determined.

(This analogue of the fundamental theorem of arithmetic has the same proof as that theorem: if also $f(x) = bq_1(x) \dots q_s(x)$, where b is constant and the $q_j(x)$ are monic and irreducible, then uniqueness is proved by Euclid's lemma and induction on $\max\{t, s\}$. One calls $F[x]$ a ***unique factorization domain*** when one wishes to call attention to this property of it.)

52. Let $f(x) = ap_1(x)^{k_1} \cdots p_t(x)^{k_t}$ and $g(x) = bp_1(x)^{n_1} \cdots p_t(x)^{n_t}$, where $k_i \geq 0, n_i \geq 0, a, b$ are nonzero constants, and the $p_i(x)$ are distinct monic irreducible polynomials (zero exponents allow one to have the same $p_i(x)$ in both factorizations). Prove that

$$\gcd(f, g) = p_1(x)^{m_1} \cdots p_t(x)^{m_t}$$

and

$$\operatorname{lcm}(f, g) = p_1(x)^{M_1} \cdots p_t(x)^{M_t},$$

where $m_i = \min\{k_i, n_i\}$ and $M_i = \max\{k_i, n_i\}$.

53. (i) Prove that the zero ideal in a ring R is a prime ideal if and only if R is a domain.

(ii) Prove that the zero ideal in a ring R is a maximal ideal if and only if R is a field.

54. The ideal I in $\mathbb{Z}[x]$ consisting of all polynomials having even constant term is a maximal ideal.

55. Let $f(x), g(x) \in F[x]$. Then $(f, g) \neq 1$ if and only if there is a field E containing both F and a common root of $f(x)$ and $g(x)$.

56. (i) Prove that if $f(x) \in \mathbb{Z}_p[x]$, then $(f(x))^p = f(x^p)$. (Hint: Use Fermat's theorem: $a^p \equiv a \bmod p$.)

(ii) Show that the first part of this exercise may be false if $\mathbb{Z}_p$ is replaced by an infinite field of characteristic p.

57. Exhibit an infinite field of characteristic p. (Hint: Exercise 20.)

58. If F is a field, prove that the kernel of any evaluation map $F[x] \to F$ is a maximal ideal.

59. If F is a field of characteristic 0 and $p(x) \in F[x]$ is irreducible, then $p(x)$ has no repeated roots. (Hint: Consider $(p(x), p'(x))$.)

60. Use Kronecker's theorem to construct a field with four elements by adjoining a suitable root of $x^4 - x$ to $\mathbb{Z}_2$.

61. Give the addition and multiplication tables of a field having eight elements. (Hint: Factor $x^8 - x$ over $\mathbb{Z}_2$.)

62. Show that a field with four elements is not (isomorphic to) a subfield of a field with eight elements.

Irreducible Polynomials

Our next project is to find some criteria for irreducibility of polynomials; this is usually difficult, and it is unsolved in general.

We begin with an elementary result, using Exercise 29: If $\sigma : R \to S$ is a ring map, then $\sigma^* : R[x] \to S[x]$, defined by

$$\sigma^* : \sum r_i x^i \mapsto \sum \sigma(r_i) x^i,$$

is also a map of rings.