MATD01 Fields and Groups

Assignment 1

Due Friday Jan 17 at 10:00 pm
(to be submitted on Crowdmark)

Notes: By a ring we always mean a commutative ring with $1 \neq 0$. For any prime number p, the field $\mathbb{Z}/p\mathbb{Z}$ is denoted by $\mathbb{F}_p$.

Please write your solutions neatly and clearly. Note that due to time limitations, only some questions will be graded. The assignment covers Chapters 2-4 of Rotman.

1. (a) Suppose $\alpha \in \mathbb{C}$ is a root of a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n \geq 1$. Show that the set

$$R = \{\sum_{i=0}^{n-1} a_i \alpha^i : a_i \in \mathbb{Q}\}$$

is a subring of $\mathbb{C}$. (Suggestion: To check that R is closed under multiplication, first note that R is certainly closed under multiplication by rational numbers. Let $f(x) = \sum_{i=0}^{n} c_i x^i$. Use the fact that $f(\alpha) = 0$ and $c_n \neq 0$ to show that α^n is in R. Now prove by induction on m that that R contains α^m for any nonnegative integer m.)

(b) Take $\alpha = \sqrt{2}$. Show that the ring $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is in fact a field. (Suggestion: Note that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$.)

2. Show that any finite integral domain is a field. (Suggestion: Given nonzero a in a finite integral domain R, consider the elements $a, a^2, a^3, \ldots$. Can they all be distinct? Make sure to mention where in your argument you are using the assumption that R is an integral domain.)

3. Let R be a ring. The smallest positive integer k such that

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}} = 0$$

is called the characteristic of R. If there is no such k, we say the ring has characteristic zero. Thus for instance, $\mathbb{Z}$ and $\mathbb{Q}$ are of characteristic zero, whereas $\mathbb{F}_p$ has characteristic p. Show that the characteristic of an integral domain is either zero or a prime number. (Suggestion: For any positive integer n, let $n_R \in R$ denote the element $1_R + 1_R + \cdots + 1_R$ with n appearances of 1_R. The distributivity axiom implies that $m_R n_R = (mn)_R$.)

4. (a) Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. By Question 1, this is a subring (actually subfield) of $\mathbb{C}$. Show that the map $\sigma : R \to \mathbb{C}$ defined by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ is a ring homomorphism. (Note that the image of σ is R as well.)

(b) Show that the only ring homomorphisms $R \to \mathbb{C}$ are the identity and σ. (Suggestion: First argue that any ring homomorphism $R \to \mathbb{C}$ must act like identity on $\mathbb{Q}$ (the key things being that 1 has to be sent to 1 and the map respects addition). Then argue that $\sqrt{2}$ can only be sent to $\pm\sqrt{2}$. Use $\sqrt{2}^2 = 2$ and the fact that a ring homomorphism respects multiplication.)

5. Let p be a prime number and R a ring of characteristic p. Show that for any $a, b \in R$,

$$(a+b)^p = a^p + b^p.$$

Conclude that the map $\phi : R \to R$ defined by $\phi(a) = a^p$ is a ring homomorphism. (Suggestion: Use the binomial formula to expand $(a+b)^p$ (which holds because of distributivity and commutativity). Note: A ring homomorphism from a ring to itself is called a ring endomorphism. The ring endomorphism ϕ of this question is called the Frobenius map.)

6. Let R be any ring. Show that there exists a unique ring homomorphism $\mathbb{Z} \to R$.

7. In each part, determine if I is an ideal of R.

(a) R any ring, a any element of R, and $I = \{ar : r \in R\}$. (The standard notation for $\{ar : r \in R\}$ is (a).)

(b) R any ring, a and b any elements of R, and $I = \{ar + bs : r, s \in R\}$. (Note: The standard notation for this is (a, b). See Question 9 of the practice list.)

(c) $R = \mathbb{Z}[x]$, and I the set of all elements of $\mathbb{Z}[x]$ in which every coefficient is a multiple of 3. (Is this a special case of Part (a)?)

(d) $R = \mathbb{Z}[x]$, and I the set of all elements of $\mathbb{Z}[x]$ in which only even powers of x appear.

Extra Practice Problems: The following problems are for your practice. They are not to be handed in for grading.

1. From the textbook: # 5, 7-16, 18-22, 26-35

2. Let $\psi : R \to S$ be a ring homomorphism. Show that the map $R[x] \to S[x]$ given by $\sum_i a_i x^i \mapsto \sum_i \psi(a_i)x^i$ is a ring homomorphism. Describe its kernel and image.

3. Let F be an integral domain of characteristic $p > 0$. Show that the map $F[x] \to F[x]$ which sends $\sum_i a_i x^i \mapsto \sum_i a_i^p x^i$ is a ring homomorphism.

4. (a) Show that the only ring homomorphism $\mathbb{Q} \to \mathbb{C}$ is the identity map.

(b) Give an example of a ring homomorphism $\mathbb{C} \to \mathbb{C}$ which is not the identity map

5. Let R be a ring. Every polynomial in $R[x]$ gives us a function $R \to R$. More precisely, given $f(x) = \sum_i a_i x^i \in R[x]$ and $\alpha \in R$, define $f : R \to R$ by $f(\alpha) = \sum_i a_i \alpha^i$. Thus to be clear about the notation, we are writing $f(x)$ for the polynomial and f for the associated function $R \to R$. Consider the map

$$\Phi : R[x] \to R^R$$

defined by $\Phi(f(x)) = f$ (see Exercise 9 of the textbook for the notation R^R). Show that Φ is a ring homomorphism, and that it will not be injective if R is finite. Give an explicit nonzero element in $\ker(\Phi)$ for $R = \mathbb{F}_p$. (Suggestion: Think about Fermat's little theorem.)

6. Let R be a ring and $\alpha \in R$. Show that the map

$$ev_\alpha : R[x] \to R$$

defined by $ev_\alpha(f(x)) = f(\alpha)$ (called evaluation at α) is a ring homomorphism. Give a nonzero element in the kernel of ev_α.

7. Show that the preimage of an ideal under a ring homomorphism is an ideal. Is the image of an ideal under a ring homomorphism always an ideal? (Prove or give a counter example.)

8. Show that a ring R is a field if and only if its only ideals are zero and R. Conclude that if F is a field, any ring homomorphism from F to any ring is injective. (In particular, if F is a finite field, any ring homomorphism $F \to F$ is an isomorphism (or an automorphism, since it goes from F to F).)

9. Let R be a ring.

(a) Show that the intersection of any collection of ideals of R is an ideal.

(b) Given any subset $S \subset R$, the intersection of all the ideals of R which contain S is called the ideal generated by S and it denoted by (S) (note that by Part (a), this is indeed an ideal). If $S = \{a_1, \ldots, a_n\}$, we just write $(a_1, \ldots, a_n)$ instead of $(\{a_1, \ldots, a_n\})$. Show that

$$(a_1, \ldots, a_n) = \{\sum_{i=1}^{n} r_i a_i : r_i \in R\}.$$

10. For any given rings R and S, we denote the set of all ring homomorphisms $R \to S$ by $\mathrm{Hom}(R, S)$. For each $\alpha \in \mathbb{C}$, let $ev_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be map given by $ev_\alpha(f(x)) = f(\alpha)$. Show that there is a bijection $\mathbb{C} \to \mathrm{Hom}(\mathbb{Q}[x], \mathbb{C})$ given by $\alpha \mapsto ev_\alpha$.

11. Show that in a ring R of characteristic $k > 0$, we have $ka = 0$ for any $a \in R$. (Here ka means $a + a + \cdots + a$, with k appearances of a. Suggestion: Use $a = 1_R a$ and distributivity.)