MATD01 Fields and Groups

Assignment 2

Due Friday Jan 24 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 $\mathbb{F}_p$. For brevity, we denote the element $r + I$ of a quotient ring R/I by $\bar{r}$.

Please write your solutions neatly and clearly. Note that due to time limitations, only some questions will be graded. The assignment covers Chapter 5 of Rotman and the division algorithm.

1. Let I and J be ideals in a ring R. Define the sum and product of I and J by

$$I + J := \{a + b : a \in I, b \in J\}$$

and

$$IJ := \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \ (1 \leq i \leq n)\}$$

(that is, IJ consists of all finite sums of elements of the form ab, with $a \in I$ and $b \in J$). Show that $I + J$ and IJ are ideals and that $I \subset I + J$ and $IJ \subset I \cap J$ (note that the intersection of any collection of ideals is an ideal, see last week's homework, Question 9 of the practice list). Give an example where $IJ \neq I \cap J$. (Hint: You should be able to get an example working with principal ideals. Note that if $I = (a)$ and $J = (b)$ then $IJ = (ab)$ (why?).)

2. (a) Let $\phi : R \to S$ be a ring map. Show that for any ideal $J \subset S$, the preimage $\phi^{-1}(J) = \{r \in R : \phi(r) \in J\}$ is an ideal of R. (That is, the preimage of an ideal under a ring map is an ideal.)

(b) Show that the image of an ideal under a surjective ring map is an ideal. (That is, if $\phi : R \to S$ is a surjective ring map, then for any ideal I of R the image $\phi(I) = \{\phi(r) : r \in I\}$ is an ideal of S.)

(c) Give an example which shows that the image of an ideal under a ring map need not be an ideal. (Hint: Consider the inclusion map $\mathbb{Z} \to \mathbb{Q}$.)

(d) Prove the correspondence theorem: if I is an ideal of a ring R, there is an inclusion-preserving 1-1 correspondence (= bijection) between the ideals of R/I and the ideals of R which contain I. (Hint: Let $\pi : R \to R/I$ be the quotient map. Show that $J \mapsto \pi^{-1}(J)$ defines a bijection

$$\Gamma : \{\text{ideals of } R/I\} \to \{\text{ideals of } R \text{ that contain } I\}.$$

Note that for this to be inclusion-preserving means $J \subset J'$ if and only if $\Gamma(J) \subset \Gamma(J')$.)

3. Let R be a ring and I an ideal of R. We say I is maximal if is a proper ideal (i.e. $I \neq R$) and moreover the only ideals of R that contain I are R and I. Show that I is maximal if and only if R/I is a field. (Hint: Think about the number of ideals of R/I. Use the correspondence theorem.)

4. Let F be a field. We say a polynomial $f(x) \in F[x]$ is irreducible (in $F[x]$) if it is of degree > 0 and cannot be factored as a product of two elements of $F[x]$ of degree > 0 (i.e. we can't express $f(x)$ as $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ of degree > 0). Suppose $f(x) \in F[x]$ is nonzero. Show that if $F[x]/(f(x))$ is an integral domain, then $f(x)$ is irreducible.

5. Let F be a field and $f(x) \in F[x]$ be nonzero. Show that every element of $F[x]/(f(x))$ can be uniquely expressed as $\overline{r(x)}$ with $r(x) = 0$ or a polynomial of degree $< \deg(f(x))$. (Hint: Division algorithm.)

6. (a) Let F be a field. By a subfield of F we mean a subring which is a field (e.g. $\mathbb{Q}$ is a subfield of $\mathbb{R}$). You can easily check that the intersection of any collection of subfields of F is a subfield. Thus there exists a smallest field contained in F, namely the intersection of all subfields of F; this smallest field is called the prime field of F. Show that the prime field of F is additively generated by 1 (that is, its underlying additive group is the subgroup $\langle 1 \rangle$ of $(F, +)$), and that the prime field is isomorphic to

$$\begin{cases} \mathbb{Q} & \text{if } \mathrm{char}(F) = 0 \\ \mathbb{F}_p & \text{if } \mathrm{char}(F) = p > 0, \end{cases}$$

where $\mathrm{char}(F)$ is the characteristic of F. (Hint: Let $\phi : \mathbb{Z} \to F$ be the canonical ring homomorphism. If ϕ is injective, show that ϕ extends to an injective ring homomorphism $\mathbb{Q} \to F$. If ϕ is not injective, consider $\ker(\phi)$. Argue that $\ker(\phi) = (p)$ where $p = \mathrm{char}(F)$. Then use the first isomorphism theorem.)

(b) Let F be a finite field of characteristic p. Show that $|F|$ (i.e. the number of elements of F) is a power of p. (Hint: Let F_0 be the prime field of F. Consider F as a vector space over F_0. Remember every vector space has a basis.)

(c) Let F be a finite field with q elements. Show that every element of F satisfies the equation $x^q - x = 0$. (Hint: Apply Lagrange's theorem (from group theory) to the group of units $F^\times$.)

7. (a) Let F be a field. Show that $F[x]/(x^2+1)$ is a field if and only if the polynomial x^2+1 has no root in F. (Hint for $\Leftarrow$: By Question 5 every element of $F[x]/(x^2+1)$ can be uniquely written as $\overline{ax+b}$ for some $a, b \in F$. Calculate $(\overline{ax+b})(\overline{-ax+b})$.)

(b) Is $\mathbb{F}_p[x]/(x^2+1)$ a field for $p = 2, 5, 13$?

(c) Construct a field with 9 elements and a field with 49 elements.

(d) Construct a field with 25 elements. (Hint: First find $c \in \mathbb{F}_5$ which does not have a square root in $\mathbb{F}_5$.)

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

1. From Galois Theory by J. Rotman, second edition: Exercises # 36-39
2. Let F be a finite field. Show that any ring homomorphism $F \to F$ is an isomorphism (or an automorphism, since it is from F to itself). (Hint: Is any ring homomorphism $F \to F$ injective?)
3. Let R be a ring and $a, b \in R$. Show that $(a) = (b)$ if and only if $a \in bR^\times$ (i.e. $a = bu$ for some unit u).
4. Is $\mathbb{Q}[x]/(x^2 - 1)$ an integral domain?
5. Show that the equation $X^2 + 1 = 0$ has two solutions in the ring $R = \mathbb{Q}[x]/(x^2 + 1)$. That is, there are two elements $\alpha, \beta \in R$ such that $\alpha^2 + 1 = \beta^2 + 1 = 0$.
6. Given rings R and S, their direct product is the cartesian product $R \times S = \{(r, s) : r \in R, s \in S\}$ with componentwise addition and multiplication (i.e. $(r, s) + (r', s') = (r + r', s + s')$ and $(r, s) \cdot (r', s') = (rr', ss')$). One can easily verify that $R \times S$ is a ring with zero $(0_R, 0_S)$ and $1 = (1_R, 1_S)$. Can $R \times S$ be an integral domain?
7. An ideal I of a ring R is called prime if $I \neq R$ and $ab \in I$ implies that a or b is in I. Show that an ideal I of R is prime if and only if R/I is an integral domain. Conclude that any maximal ideal is prime.
8. Let R be a ring of characteristic 0 (thus the canonical map $\mathbb{Z} \to R$ is injective). Classify all ring homomorphisms $\mathbb{Q}[x] \to R$. (Hint: There is a unique ring map $\mathbb{Q} \to R$. To extend this to a ring map $\mathbb{Q}[x] \to R$ think about the image of x.)