MATD01 Fields and Groups

Assignment 4

Due Friday Feb 7 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 $\bar{r}$. Given rings R and S, we denote the set of all ring homomorphisms $R \to S$ by $\mathrm{Hom}(R, S)$.

Please write your solutions neatly and clearly. Note that due to time limitations, only some questions will be graded.

1. Determine if each statement below is true or false. You don't have to include any explanation in your submission, but make sure that you know why each statement is true or false (i.e. you know the proof if the statement is true and a counter-example if the statement is false).

(a) The composition of two ring homomorphisms is a ring homomorphism.
(b) Let $\phi : S \to T$ be a ring homomorphism and R a subring of S. Define $\phi|_R : R \to T$ (read the restriction of ϕ to R) by $\phi|_R(r) = \phi(r)$. Then $\phi|_R$ is a ring homomorphism.
(c) If F is a field and R any ring, then any ring homomorphism $F \to R$ is injective.
(d) If F is a field and R any ring, then any surjective ring homomorphism $F \to R$ is an isomorphism.

In statements (e)-(l) below R is a ring, $a, b \in R$, and I is an ideal of R.

(e) If $a = bu$ with $u \in R^\times$, then $(a) = (b)$.
(f) If $(a) = (b)$ and R is an integral domain, then $a = bu$ for some $u \in R^\times$.
(g) If a is irreducible and $b \mid a$, then either $(b) = (a)$ or $(b) = R$.
(h) If R is an integral domain and a is irreducible, then (a) is maximal. (Do Problem 7 first.)
(i) If R is an integral domain and a is irreducible, then (a) is prime. (Do Problem 7 first.)
(j) If a is irreducible, then so is au for any unit u.
(k) An ideal I is prime if and only if R/I is an integral domain.
(l) An ideal I is maximal if and only if R/I is a field.
(m) Any maximal ideal is prime.
(n) Zero is a prime ideal of a ring R if and only if R is an integral domain.
(o) Any generator of a nonzero prime principal ideal is irreducible.
(p) If R is an integral domain, any nonzero prime ideal of R is maximal. (Hint: Consider the ideal (x) in $\mathbb{Z}[x]$.)
(q) In a PID, a nonzero ideal I is prime if and only if it is maximal if and only if $I = (a)$ for some irreducible a.
(r) If F is a field and $f(x) \in F[x]$ is irreducible, then $F[x]/(f(x))$ is a field.
(s) If $F \subset K$ are fields and $f(x) \in F[x]$ is irreducible in $F[x]$, then $f(x)$ is also irreducible in $K[x]$. (Hint: Think about $x^2 - 2$ in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.)
(t) $\mathbb{R}/(x^2 + 1)$ is isomorphic to $\mathbb{C}$ and $\mathbb{R}/(x - \pi)$ is isomorphic to $\mathbb{R}$. (Hint: Use the first isomorphism theorem.)

(u) If F is a field, any nonzero ideal of $F[x]$ has a unique monic generator.
(v) If F is field, a polynomial $f(x) \in F[x]$ of degree 2 or 3 is irreducible if and only if it does not have a root in F.

2. Let R be a PID and $a, b, c \in R$. Suppose a and b are relatively prime. Show that if a and b divide c, then so does ab. Conclude that $(a) \cap (b) = (ab)$. (Recall that we say a, b are relatively prime if $(a, b) = R$.)

3. Let R and S be rings. Define a bijection between $\mathrm{Hom}(R[x], S)$ and the cartesian product

$$\mathrm{Hom}(R, S) \times S = \{(\phi, \alpha) : \phi \in \mathrm{Hom}(R, S), \alpha \in S\}.$$

4. Consider the ideal $I = (2, x)$ of $\mathbb{Z}[x]$. Show that I is not principal. (Thus the integral domain $\mathbb{Z}[x]$ is not a PID.)

5. (a) Factor the polynomial $x^6 - 1 \in \mathbb{Q}[x]$ as a product of irreducible polynomials.

(b) Let ω be a primitive complex 6th of unity. That is, $\omega \in \mathbb{C}$ is a root of $x^6 - 1$, but is not a root of $x^k - 1$ for any $1 \leq k < 6$. Find the minimal polynomial of ω over $\mathbb{Q}$. (Recall that the minimal polynomial of ω over $\mathbb{Q}$ is the the unique monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\omega) = 0$. See last week's assignment.)

(c) What is the kernel of the map $\mathbb{Q}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(\omega)$? (Your answer will be like "the kernel is the ideal generated by ...")

(d) Show that $f(x) = x^m + x^n + 1$ is not irreducible over $\mathbb{Q}$ if $m \equiv 2 \pmod 6$ and $n \equiv 4 \pmod 6$. (Hint: Calculate $f(\omega)$.)

6. We will soon show that the polynomial $f(x) = \sum_{i=0}^{6} x^i$ is irreducible in $\mathbb{Q}[x]$ (in fact, we will see that $\sum_{i=0}^{p-1} x^i$ is irreducible in $\mathbb{Q}[x]$ for any prime p). Thus $\mathbb{Q}[x]/(f(x))$ is a field. Let $g(x) = x^2 + 1$. Find $\overline{g(x)}^{-1}$ in $\mathbb{Q}[x]/(f(x))$. (Hint: Euclid's algorithm can be helpful.)

7. Recall that if R is a PID and $a \in R$ is irreducible, then $a \mid bc$ implies that $a \mid b$ or $a \mid c$ (or in other words, $bc \in (a)$ implies that $b \in (a)$ or $c \in (b)$). The goal of this question is to show that this statement need not be true in a general integral domain.

Let D be a positive integer. Let $\sqrt{-D} \in \mathbb{C}$ be a square root of $-D$ in $\mathbb{C}$ (that is, a complex root of $x^2 + D$). Let $\mathbb{Z}[\sqrt{-D}]$ be the image of the ring map $ev_{\sqrt{-D}} : \mathbb{Z}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(\sqrt{-D})$.

(a) Show that $\mathbb{Z}[\sqrt{-D}]$ is the set of $\mathbb{Z}$-linear combinations of 1 and $\sqrt{-D}$ (that is, $\mathbb{Z}[\sqrt{-D}] = \{a + b\sqrt{-D} : a, b \in \mathbb{Z}\}$).

(b) Show that $\mathbb{Z}[\sqrt{-D}]^\times = \{1, -1, \sqrt{-D}, -\sqrt{-D}\}$ if $D = 1$ and $\mathbb{Z}[\sqrt{-D}]^\times = \{1, -1\}$ if $D > 1$.

(c) Now we specialize to $D = -5$. Show that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. (Remark: Note that not every prime integer remains irreducible in $\mathbb{Z}[\sqrt{-5}]$: $41 = (6 + \sqrt{-5})(6 - \sqrt{-5})$.)

(d) Check that 2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$, but it does not divide any of $1 \pm \sqrt{-5}$. (Thus in the ring $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible but the ideal (2) is not prime.)

(e) Is $\mathbb{Z}[\sqrt{-5}]$ a PID?

Remark: The ring $\mathbb{Z}[\sqrt{-5}]$ is not even a UFD: $6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and $2, 3, 1 \pm \sqrt{-5}$ are all irreducible so that 6 can be factored as a product of irreducibles in more than one way.

Bonus credit question. Let R be a ring. Define a group structure on $\{(\alpha, \beta) \in R^2 : \alpha^2 + \beta^2 = 1\}$. (This question is not necessarily related to what we have been doing in the course lately. Please hand in separately in physical form, in class or office hours.)

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 # 49-55

2. (a) Let R be a ring of positive characteristic. Show that there is no ring homomorphism $\mathbb{Q} \to R$.

(b) Let F be a field of characteristic zero. Show that there is a unique ring homomorphism $\mathbb{Q} \to R$.

3. Show that $\mathbb{Z}[x]/(n, x)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Conclude that the ideal (p, x) of $\mathbb{Z}[x]$ is maximal if p is a prime number.

4. Show that any quotient of a PID is a PID.

5. (a) Let R be a PID and $a, b \in R$ relatively prime. Show that $R/(ab) \simeq R/(a) \times R/(b)$. (See Problem 6 of the practice list of Assignment 2 for the definition of the right hand side.)

(b) Show that $\mathbb{Q}[x]/(x^2 - 1) \simeq \mathbb{Q}^2$.

6. Consider the ring $\mathbb{Z}[x, y]$ of polynomials in two variables x, y and with coefficients in $\mathbb{Z}$ (with the obvious addition and multiplication, e.g. $(ax + bxy^2)(cy + dx^2) = acxy + adx^3 + bcxy^3 + bdx^3y^2$ for any $a, b, c, d \in \mathbb{Z}$). Let $f(x, y) \in \mathbb{Z}[x, y]$ and $I = (f(x, y))$. Given any ring R, construct a 1-1 correspondence (bijection) between $\mathrm{Hom}(\mathbb{Z}[x, y]/I, R)$ and the set $\{(\alpha, \beta) \in R^2 : f(\alpha, \beta) = 0\}$.

7. (a) Let $\omega \in \mathbb{C}$ be a primitive third root of unity, i.e. $\omega^3 = 1$ but $\omega, \omega^2 \neq 1$. Find the minimal polynomial of ω.

(b) Is the polynomial $x^5 + x^4 + 1$ irreducible in $\mathbb{Q}[x]$? If not, factor it as a product of irreducible polynomials.

8. (Challenge question, won't be tested.) Let R be a ring. The ring of power series $R[[x]]$ with coefficients in R is defined as follows: the elements are formal sums $\sum_{n=0}^{\infty} a_n x^n$ with the a_n in F, with possibly infinitely many of the a_n nonzero. Addition and multiplication are defined in the natural way (like power series in calculus). Show that if F is a field, $F[[x]]$ has a unique maximal ideal.