MATD01 Fields and Groups

Assignment 3

Due Friday Jan 31 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. The assignment covers up to Chapter 6 of Rotman.

1. Let p be a prime number and F a field with $q = p^k$ elements. Prove that

$$x^{q-1} - 1 = \prod_{\alpha \in F^\times} (x - \alpha)$$

in $F[x]$. By comparing coefficients of suitable powers of x, conclude that (i) $\sum_{\alpha \in F^\times} \alpha = 0$ and (ii) $\prod_{\alpha \in F^\times} \alpha = -1$. (Remark: Note that in particular, if we take $F = \mathbb{F}_p$, (ii) gives Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. Hint: Think about the roots of $x^{q-1} - 1$ in F. A question from last week's assignment can be useful. Also the following result can be useful: if $f(x) \in F[x]$ has distinct roots $\alpha_1, \ldots, \alpha_n \in F$, then $\prod_{i=1}^{n} (x - \alpha_i) \mid f(x)$.)

2. An element r of a ring R is called irreducible if it satisfies the following two properties: (i) r is not a unit, and (ii) if $r = ab$ for some $a, b \in R$, then a or b is a unit.

(a) Suppose R is an integral domain and $r \in R$ nonzero. Show that if the ideal (r) is maximal, then r is irreducible. (Recall that an ideal I of R is called maximal if $I \neq R$ and there is no ideal J such that $I \subsetneq J \subsetneq R$.)

(b) Show that if R is a PID then the converse of the statement of the previous part is also true. That is, if r is irreducible, then (r) is maximal.

(c) Construct a field with 4 elements. (Hint: Find an irreducible polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 2. Keep Question 3 of last week's assignment in mind.)

3. Let $F \subset K$ be fields. Let $\alpha \in K$. We say α is algebraic over F if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. For instance, every element of F is algebraic over F (α being a root of $x - \alpha$).

(a) True or false: α is algebraic over F if and only if the map $ev_\alpha : F[x] \to K$ given by $f(x) \mapsto f(\alpha)$ is not injective.

(b) Suppose α is algebraic over F. Let $f(x) \in \ker(ev_\alpha)$. Show that $f(x)$ is irreducible if and only if it generates $\ker(ev_\alpha)$. Conclude that there is a unique monic irreducible polynomial $p_\alpha(x) \in F[x]$ such that $p_\alpha(\alpha) = 0$. The polynomial $p_\alpha(x)$ is called the minimal polynomial of α over F.

(c) Find the minimal polynomials of i and $\sqrt{2} + 1$ over $\mathbb{Q}$ and $\mathbb{R}$.

(d) We say K is a finite extension of F if K is finite dimensional as a vector space over F. Show that if K is a finite extension of F, then every element of K is algebraic over F. (Hint:

Let n be the dimension of K as a vector space over F. Given $\alpha \in K$, consider the elements α^j $(0 \leq j \leq n)$. Can they be linearly independent?)

4. (a) Find all ring homomorphisms $\mathbb{Q}[x] \to \mathbb{C}$. (Hint: Is such a homomorphism determined by the image of x?)

(b) Let R and S be rings and I an ideal of R. Let $\pi : R \to R/I$ be the quotient map. Let $\phi : R \to S$ be a ring homomorphism. Show that $I \subset \ker(\phi)$ if and only if there is a ring homomorphism $\overline{\phi} : R/I \to S$ such that $\phi = \overline{\phi} \circ \pi$. Moreover, show that the map $\overline{\phi}$ is unique when it exists. Conclude that we have a bijection

$$\{\phi \in \mathrm{Hom}(R, S) : I \subset \ker(\phi)\} \ \to\ \mathrm{Hom}(R/I, S)$$

given by $\phi \mapsto \overline{\phi}$. (See the notes at the beginning for the notation $\mathrm{Hom}(R, S)$.)

(c) Find all ring homomorphisms $\mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C}$ and $\mathbb{Q}[x]/(x^3 - 2) \to \mathbb{R}$ and the kernel and image of each. Are the images fields? (Hint: Is $x^3 - 2$ irreducible in $\mathbb{Q}[x]$?)

(d) Find all ring homomorphisms $\mathbb{Q}[x]/(x^3 - 8) \to \mathbb{C}$ and the kernel and image of each.

5. (a) Use Euclid's algorithm to find the gcd of the elements $f(x) = x^{10} - 1$ and $g(x) = x^6 - 1$ of $\mathbb{Q}[x]$. Give a generator for the ideal $(f(x), g(x))$ of $\mathbb{Q}[x]$.

(b) What is the gcd of the polynomials $f(x)$ and $g(x)$ of Part (a) considered as elements of $\mathbb{C}[x]$?

(c) Write $g(x)$ as a product of ireducible polynomials in (i) $\mathbb{Q}[x]$ and (ii) $\mathbb{C}[x]$.

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 # 40-48
2. Find the kernel of the map $\phi : \mathbb{Q}[x] \to \mathbb{C}$ defined by $f(x) \mapsto f(i)$. (Hint: Question 3 of the assignment.)
3. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Show that

$$F := span_{\mathbb{Q}}\{\alpha^j : j \geq 0\}$$

(i.e. the set of all linear combinations of the α^j ($j \geq 0$) with coefficients in $\mathbb{Q}$) is a subfield of $\mathbb{C}$, and that $\dim_{\mathbb{Q}}(F)$ (i.e. the dimension of F as a vector space over $\mathbb{Q}$) equals the degree of the minimal polynomial of α over $\mathbb{Q}$. (Hint: To see F is a field, consider the evaluation map $ev_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ (sending $f(x) \mapsto f(\alpha)$). What are its image and kernel? Use the first isomorphism theorem. Remember the minimal polynomial of α over $\mathbb{Q}$ is irreducible in $\mathbb{Q}[x]$. For the assertion regarding the dimension, try to give a basis of F.)
4. Let R be a ring.

(a) Show that if $a, b \in R$ are irreducible and $a \mid b$, then $b = au$ for a unit u (and hence $(a) = (b)$).

For the remainder of this question we assume R is a PID.

(b) We say $a, b \in R$ are relatively prime if $(a, b) = R$. Show that if a and b are relatively prime and $a \mid bc$, then $a \mid c$.

(c) Let a be irreducible. Show that given any $b \in R$, either $a \mid b$ or a and b are relatively prime. Conclude that if $a \mid bc$ (and a is irreducible), then $a \mid b$ or $a \mid c$.

5. Let R be a ring. A collections of ideals $(I_n)_{n\geq 0}$ of R with

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

is called an ascending chain of ideals. An ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ is said to stabilize, or eventually become stationary, if there is some positive integer N such that $I_n = I_{n+1}$ for $n \geq N$. The ring R is called Noetherian* if any ascending chain of ideals of R stabilizes.

(a) Show that any PID is Noetherian. (Hint: Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals in a principal ideal domain R. Consider the union $J = \bigcup_{n\geq 1} I_n$. Is J an ideal (why)? Now use the assumption that R is a PID.)

(b) Let R be a PID. Let $r \in R$ be nonzero and not a unit. Show that r is divisible by an irreducible element. (Hint: Suppose not (so in particular, r is not irreducible itself). Try to produce an ascending chain of ideals that does not stabilize.)

(c) An integral domain R is called a unique factorization domain (or a UFD, for short) if it satisfies the following property: if $r \in R$ is nonzero and not a unit, then (i) $r = a_1 \ldots a_k$ for some irreducible elements $a_1, \ldots, a_k$, and (ii) if $r = a_1 \ldots a_k$ and $r = b_1 \ldots b_\ell$ with the a_i and b_j irreducible, then $k = \ell$ and moreover, after possibly relabelling the b_j, we have $a_i \in b_i R^\times$. (In other words, the factorization is "as unique as it can be", that is, up to rearranging the factors and rescaling by units.)

An example of a unique factorization domain is $\mathbb{Z}$; this is by the fundamental theorem of arithmetic. Show that any PID is a UFD.

*Named after Emmy Noether (1882-1935).

6. Let R be a 3-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \beta\}$. Thus every element of R is a formal linear combination $a + b\alpha + c\beta$ with $a, b, c \in \mathbb{Q}$, with addition and scalar multiplication defined in the obvious way (that is, $(a + b\alpha + c\beta) + (a' + b'\alpha + c'\beta) = (a + a') + (b + b')\alpha + (c + c')\beta$ and $r(a + b\alpha + c\beta) = ra + rb\alpha + rc\beta$). There is an obvious way of identifying $\mathbb{Q}$ as a subset of R (namely, by $a \mapsto a + 0\alpha + 0\beta$). Define a multiplication on R which makes it a field with $\mathbb{Q} \subset R$ a subfield. (Hint: You need to define α^2, $\alpha\beta$, and β^2 appropriately. First use quotient rings to construct a field extension F of $\mathbb{Q}$ which is three dimensional as a vector space over $\mathbb{Q}$. Then "transport" the multiplication from F to R.)

7. 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.