ALGEBRA III, AUG-DEC 2017. PROBLEM SETS

MANOJ KUMMINI

INSTRUCTIONS

(1) Write carefully. Points will be taken off for ambiguous statements.
(2) Use proper quantifiers, when needed.
(3) The universal quantifier should be stated as "for every" or "for all" or "$\forall$". For example, we say that x^2 is positive *for every real number x* (or, *for all real numbers x*).
(4) The existential quantifier is "there exists" ("there exist" in plural) or $\exists$. For example, for every positive real number x, there exist exactly two real numbers y such that $y^2 = x$.
(5) Avoid using 'for any', 'any' etc in quantifiers at all costs.
(6) 'Therefore', 'so', 'hence' etc. mean implication.

NOTATION

(1) R and S denote commutative rings with $1 \neq 0$, unless otherwise specified. Even when we consider non-commutative rings, we will assume that they have a 1 that is not equal to 0.
(2) $\Bbbk$ and F denote fields.

1. SET 1: DUE 2017-AUG-17

1.1. Let R be not necessarily commutative. Let $r, s, s' \in R$. Show that if $rs = sr = 1$ and $rs' = s'r = 1$, then $s = s'$. (Conclusion: If R is an element, then there exists a unique $s \in R$ such that $rs = sr = 1$, called *the inverse* of r.)

1.2. Let R be not necessarily commutative. The set of invertible elements of R form a group under multiplication, usually denoted $R^\times$.

1.3. Check that the map $\rho_r : R \longrightarrow R, s \mapsto sr$ is a group homomorphism of $(R, +)$ to $(R, +)$.

1.4. Let $e \in R$ be an element such that $e^2 = e$ and $e \notin \{0, 1\}$. (Such elements are called *idempotent elements*.) Show that the map $R \longrightarrow R\ r \mapsto re$ satisfies the first two properties in our definition of ring homomorphisms, but not the third.

1.5. Let X be a set, and $P(X)$ the power set of X, i.e., the set of subsets of X. For $A, B \in P(X)$, define

$$A + B = (A \smallsetminus B) \cup (B \smallsetminus A)$$

and

$$A \cdot B = A \cap B.$$

Show that $P(X)$ is a commutative ring with $1 = X$ and $0 = \varnothing$. Show that every element of $P(X)$ is idempotent.

1.6. Let R be not necessarily commutative. Suppose that every element of R is idempotent. Show that R is commutative. (Hint. For $r, s \in R$, expand $(r + s)^2$.)

1.7. Chapter 11, p.354, Exercise 1.7(b).

1.8. An element $r \in R$ is called *nilpotent* if there exists an integer $n \geq 0$ such that $r^n := \underbrace{rr \cdots r}_{n \text{ times}} = 0$. Show that if r is nilpotent, then $1 + r$ is invertible.

2. Set 2: Due 2017-Aug-29

2.1. Recall that a subring S of R is a subset that is an abelian subgroup of R under addition (of R), is closed under the multiplication of R and contains 1_R. Show that if S is a subring of R, then it is a ring with addition and multiplication inherited from R.

2.2. It is possible for R to have a subset S that is also a ring (with its own addition, multiplication and 1_S) but not a subring of R. Let R be the ring of 2×2 real diagonal matrices and

$$S = \left\{ \begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix} \mid r \in \mathbb{R} \right\}.$$

Then S is ring (with addition and multiplication inherited from R) but not a subring of R ($1_S \neq 1_R$).

2.3. Let $S \subseteq R$ be rings (i.e., they both are rings on their own, but S is not necessarily a subring, i.e., the operations in S or its additive/multiplicative identies need not be compatible with R). There is a natural function $\iota : S \longrightarrow R$, given by inclusion. Show that S is a subring of R if and only if ι is a ring homomorphism. (Hint: e.g., the statement $\iota(1_S) = 1_R$ is another way of saying that S and R have the same multiplicative identity.)

2.4. Let $a_1, \ldots, a_n \in \mathbb{Z}$. Show that the smallest ideal of $\mathbb{Z}$ that contains a_i, for all i, is generated by $\gcd\{a_1, \ldots, a_n\}$, i.e., it is the set of all the multiples of the gcd. (Hint: try $n = 2$ first, and see if you can use induction.)

2.5. Let I and J be R-ideals. Show that $I \cap J$ is an R-ideal. Show examples of $\mathbb{Z}$-ideal I and J such that $I \cup J$ is *not* a $\mathbb{Z}$-ideal.

2.6. Chapter 11, p.354, Exercises 1.1 (Definition: An *algebraic number* is a complex number that satisfies a polynomial equation with rational coefficients.); 1.3; 1.6.

2.7. Let R be a ring and S a subring of R. Let $r \in R$. Show that $S[r]$ is the smallest subring of R containing S and r.

2.8. For a subset A of R, define the *ideal generated by A* to be

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, r_i \in R \text{ and } a_i \in A \text{ for all } 1 \leq i \leq n \right\},$$

the set of all the *finite* R-linear combinations of the elements of A. (In the class, we saw this definition when A is finite.) Show that the ideal generated by A is the smallest ideal containing A.

2.9. For R-ideals I and J, define $I + J$ to be the set $\{a + b \mid a \in I, b \in J\}$. Show that $I + J$ is an ideal and that it is the ideal generated by $I \cup J$.

3. Set 3: Due 2017-Sep-05

3.1. Show that for a subset A of R, the ideal generated by A is the intersection of all the ideals containing A.

3.2. Show that the characteristic of a domain is zero or a prime number.

3.3. Prove Proposition 11.2.9 (Hint: induct on the degree of f.) and read Corollaries 11.2.10 and 11.2.11.

3.4. Let R be a PID and f, g be nonzero elements of R. Show that there exists $e \in R$ such that

(1) e divides f and g;
(2) for every $d \in R$, if d divides f and g, then d divides e.
(3) $e = af + bg$ for some $a, b \in R$.

(Recall definition: r divides s if $s \in (r)$. Warning: As such we cannot impose any uniqueness condition on e. In $\mathbb{Z}$, we can take such an e to be a positive to make it unique; in a polynomial ring over a field, we can take it to be monic to make it unique.)

4. Set 4: Due 2017-Sep-21

4.1. Let $r \in R$ be a nilpotent element. Show that $1 + rX$ is invertible in the polynomial ring $R[X]$.

4.2. Let R be a domain. Show that the invertible elements of the polynomial ring $R[X]$ are exactly the constant polynomials given by the invertible elements of R.

4.3. Let $f(X) \in R[X]$. An element $r \in R$ is said to be a *root* of $f(X)$ if $f(r) = 0$. Show that r is a root of $f(X)$ if and only if $f(X) \in (X - r)$. (Hint Consider the ring homomorphism $R[X] \longrightarrow R, g(X) \longrightarrow g(r)$.) Definition: The *multiplicity* of a root r of $f(X)$ is the largest integer n such that $f(X) \in (X - r)^n$. A root r of $f(X)$ is said to be a *simple* root of $f(X)$ if its multiplicity is 1, and a *multiple* root if the multiplicity if greater than 1.

4.4. Chapter 11, Exercises 2.2; 3.3(a), (b), (d), (e); 3.4; 3.5; 3.6; 3.8; 3.9(b); 3.10; 3.11; 4.3 (all)

5. Set 5: Due 2017-Nov-09

5.1. Chapter 11 Exercises 7.1; 7.3; 8.2; 8.3; 9.1; 9.8;

5.2. Chapter 12 Exercises 2.1; 2.4; 2.10; 3.2; 3.4; 3.5 (skip the bit about 'variety'); 4.1; 4.2; 4.3;

5.3. Chapter 15 Exercises 1.1;

5.4. Let R be a ring. The *prime subring* of R is the image of the unique homomorphism $\mathbb{Z} \longrightarrow R$. Show that if R is a field, then its prime subfield is the field of fractions of its prime subring.

6. Set 6: For the quiz on 2017-Nov-21

6.1. Chapter 15 Exercises 1.2; 2.1; 3.1; 3.3; 3.9; 3.10; 6.1; 7.1; 7.3; 7.5; 10.1

Chennai Mathematical Institute, Siruseri, Tamilnadu 603103. India
E-mail address: mkummini@cmi.ac.in