Math 3613

Solutions to Second Exam

November 22, 2013

1. Definitions

(a) (4 pts) What precisely do we mean when we say a is *congruent to b modulo n* (i.e. $a \equiv b \pmod{n}$)?

- a is *congruent to b modulo n* means the difference $a - b$ is an integer multiple of n.

(b) (5 pts) Suppose R is a set with two operations defined: "addition" $\oplus : R \times R \to R$ and "multiplication" $\otimes : R \times R \to R$ and "multiplication". What additional properties are required so that R is a ring? (Hint: there are six additional required properties.)

- $a + b = b + a$ for all $a, b \in R$ (commutativity of addition)
- $a + (b + c) = (a + b) + c$, for all $a, b, c \in R$ (associativity of addition)
- There exists $0_R \in R$ such that $a + 0_R = a$ for all $a \in R$ (existence of an additive identity)
- For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0_R$ (existence of additive inverses)
- For each $a, b, c \in R$, $a(bc) = (ab)\,c$ (associativity of multiplication)
- For each $a, b, c \in R$, $a\,(b + c) = (ab) + (ac)$ (distributativity of multiplication over addition)

(c) (4 pts) What is an *integral domain*?

- a non-zero commutative ring with identity and without any zero divisors.

(d) (4 pts) What is a *homomorphism* between two rings?

- a mapping $f : R \to S$ between two rings such that for all $r, r' \in R$, one has both $f\,(r +_R r') = f\,(r) +_S f\,(r')$ and $f\,(r \times_R r') = f\,(r) \times_S f\,(r')$.

(e) (4pts) What is the *greatest common divisor* of two polynomials over a field F?

- The monic polynomial of highest degree that divides both f and g.

(f) (4pts) What is an *irreducible polynomial*?

- a nonconstant polynomial f whose only divisors are the non-zero constants and the associates of f.

Due to a typo in numbering there was no problem 2 on the exam.

3. (15 pts) Suppose $GCD(a,n) = 1$. Prove that $[a]_n$ is a unit in $\mathbb{Z}_n$.

- By Theorem 1.3, there exist integers u and v such that
$$1 = GCD(a,n) = ua + nv \quad \Rightarrow \quad ua - 1 = nv$$
If we now descend to congruence classes modulo n
$$ua - 1 = nv \quad \Rightarrow \quad [ua-1]_n = [nv]_n \quad \Rightarrow \quad [u]_n [a]_n - [1]_n = [0]_n \quad \Rightarrow \quad [u]_n [a]_n = [1]_n$$
and so $[a]_n$ is a unit in $\mathbb{Z}_n$.

4 . (15 pts) Suppose S is a nonempty subset of a ring R such that

(i) $$a - b \in S \quad \text{for all } a, b \in S$$

(ii) $$ab \in S \quad \text{for all } a, b \in S$$

Show that S is a subring of R.

- So that we can invoke Theorem 3.3, we need to show (a) $a + b \in S$ for all $a, b \in S$, (b) $ab \in S$ for all $a, b \in S$ and (c) $a \in S$ implies $-a \in S$. (b) is already identical to (ii). So we just need to show that (i) implies (a) and (c).
Step 1. Show $0_R \in S$. Choose $b = a$ in (i). Then
$$a - a \in S \quad \Rightarrow \quad 0_R \in S$$
Step 2. Show if $b \in S$, then $-b \in S$. Choose $a = 0_R \in S$ (valid by Step 1). (This step verifies (c).)
$$0_R - b \in S \quad \Rightarrow \quad -b \in S$$
Step 3. Show $a + b \in S$. By Step 2, $b \in S \quad \Rightarrow \quad -b \in S$, and so by assumption (i),
$$a - (-b) \in S \quad \Rightarrow \quad a + b \in S$$
verifiying (a).

5. (15 pts) Let R and S be rings and $f : R \to S$ a ring homomorphism. Prove that
$$f(R) = \{s \in S \mid s = f(r) \text{ for some } r \in R\}$$
is a subring of S.

- We need to verify the three properties of a subring (as in Theorem 3.3). Suppose $s, s' \in f(R)$. Then $s = f(r)$ for some $r \in R$ and $s' = f(r')$ for some $r' \in R$.
$$\begin{aligned} s + s' = f(r) + f(r') = f(r + r') &\qquad \text{because } f \text{ is a ring homomorphism} \\ \Rightarrow \quad s + s' \in S \quad \Rightarrow &\quad \text{closure under addition} \end{aligned}$$
$$\begin{aligned} s \cdot s' = f(r) \cdot f(r') = f(r \cdot r') &\qquad \text{because } f \text{ is a ring homomorphism} \\ \Rightarrow \quad s \cdot s' \in S \quad \Rightarrow &\quad \text{closure under multiplication} \end{aligned}$$
$$\begin{aligned} -s = -f(r) = f(-r) &\quad \text{by Theorem 3.11 (ii)} \\ \Rightarrow \quad S &\text{ is closed under taking additive inversse.} \end{aligned}$$

6. (15 pts) Let F be a field and $f, g \in F[x]$. Prove that f and g are associates if and only if $f|g$ and $g|f$.

- $\Rightarrow$ Suppose f and g are associates. Then by definition, there exists a nonzero constant $c \in \mathbb{F}$ such that
$$g = cf \quad \Rightarrow \quad f|g$$
$$g = cf \quad \Rightarrow \quad f = c^{-1}g \quad \Rightarrow \quad g|f$$
- $\Longleftarrow$ Suppose $f|g$ and $g|f$. Then there exist polynomials s and t such that
$$f = sg \qquad \text{and} \qquad g = tf$$
If we take degrees on both sides of these equations (using Theorem 4.1)
$$\deg(f) = \deg(s) + \deg(g) \quad \Rightarrow \quad \deg(f) \leq \deg(g)$$
$$\deg(g) = \deg(t) + \deg(f) \quad \Rightarrow \quad \deg(g) \leq \deg(f)$$
But then if both these inequalities are to be satisfied, we must have $\deg(f) = \deg(g)$, and so $\deg(s) = \deg(t) = 0$. That means s and t are constants, and so f and g are associates.

7. (15 pts) Let $\mathbb{F}$ be a field and let $f, g, h \in \mathbb{F}[x]$ with f and g relatively prime. Suppose further $f \mid h$ and $g \mid h$. Show that $(fg) \mid h$.

- Since f and g are relatively prime, by Theorem 4.4 there exists polynomials u and v such that
$$1 = GCD(f, g) = uf + vg.$$
Multiplying the extreme sides of this equation by h we get
$$h = ufh + vgh \tag{*}$$
Next, we note
$$f|h \quad \Rightarrow \quad h = sf \quad \text{for some polynomial } s$$
$$g|h \quad \Rightarrow \quad h = tg \quad \text{for some polynomal } t$$
We can thus substitute for h in two different way on the right hand side of (*) to get
$$h = uf(tg) + vg(sf) = (ut + vs)(fg) \quad \Rightarrow \quad (fg)|h$$