MATH 258: Homework #4

Jesse Farmer

02 February 2005

1. *Let p be prime. Show that p divides $\binom{p}{i}$ for $1 \le i \le p-1$. Deduce that for x, y elements of a commutative ring A of characteristic p, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.*

   Lemma 1. *If a, b, c are integers with $c \mid ab$ where a and c are relatively prime then $c \mid b$.*

   Proof. Since a and c are relatively prime there exist integers j and k such that

   $$cj + ak = 1$$

   And hence

   $$cbj + abk = b$$

   By hypothesis there exists an integer h such that $ab = hc$ and therefore

   $$c(bj + hk) = b$$

   □

   Since $\binom{p}{i}$ is an integer and

   $$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

   we have $i! \mid p(p-1)\cdots(p-i+1)$. But g.c.d$(p, i!) = 1$ since $1 \le i \le p-1$. From the above lemma, $i! \mid (p-1)\cdots(p-i+1)$, and hence

   $$\binom{p}{i} = p \cdot \frac{(p-1)\cdots(p-i+1)}{i!} = pk$$

   where k is an integer.

   Let $x, y \in A$ where A is a commutative ring with char $A = p$ for some prime p. Then

   $$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot x^k y^{p-k}$$

   For $1 \le k \le p-1$ and some $j \in \mathbb{Z}$

   $$\binom{p}{k} = pj = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ times}} j = 0$$

   since char $A = p$. Hence $\binom{p}{k} x^k y^{p-k} = 0$ for all $1 \le k \le p-1$ and $(x+y)^p = x^p + y^p$. Assume $(x+y)^{p^n} = x^{p^n} + y^{p^n}$. Then

   $$(x+y)^{p^{n+1}} = \left((x+y)^{p^n}\right)^p = \left(x^{p^n} + y^{p^n}\right)^p = \left(x^{p^n}\right)^p + \left(y^{p^n}\right)^p = x^{p^{n+1}} + y^{p^{n+1}}$$

   Therefore $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for all $n \in \mathbb{N}$.

2. *Determine the ideals, prime ideals, and maximal ideals of* $\mathbb{Z}/168\mathbb{Z}$.

   There is a one-to-one correspondence between ideals of $\mathbb{Z}/168\mathbb{Z}$ and ideals of $\mathbb{Z}$ that contain $168\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, any ideal which contains $168\mathbb{Z}$ must be of the form $k\mathbb{Z}$ where $k \mid 168$. The maximal ideals are those that correspond to the prime divisors of 168. The ideals are therefore all $(k\mathbb{Z})/(168\mathbb{Z})$ where $k \mid 168$, and the maximal ideals (and prime ideals) are all such k that are prime, namely, $k = 2, 3, 7$.

3. *Let p be a prime. Show that $\mathbb{Q}(\sqrt{p})$ is a field. Find all q prime such that $\mathbb{Q}(\sqrt{p}) \cong \mathbb{Q}(\sqrt{q})$.*

   Since addition is performed coordinate-wise $\mathbb{Q}(\sqrt{p})$ is clearly an abelian group with respect to addition. Consider $(\mathbb{Q}(\sqrt{p}), \cdot)$. We will treat $\mathbb{Q}(\sqrt{p})$ as a subset of $\mathbb{Q} \times \mathbb{Q}$ with multiplication defined by

$$(a, b) \cdot (c, d) = (ac + pbd, ad + bc)$$

$$\begin{aligned}
(a, b)((c, d)(e, f)) &= (a, b)(ce + pdf, cf + de) \\
&= (ace + padf + pbcf + pbde, acf + ade + bce + pbdf) \\
&= (ac + pbd, ad + bc)(e, f) \\
&= ((a, b)(c, d))(e, f)
\end{aligned}$$

   The identity is $(1, 0)$: $(a, b)(1, 0) = (a + pb0, a0 + b) = (a, b)$, and the operation is commutative since addition and multiplication on $\mathbb{Q}$ are commutative. The inverse of $(a, b) \neq 0$ is given by

$$(a, b) \cdot \left(\frac{a}{a^2 - pb^2}, \frac{-b}{a^2 - pb^2} \right) = \left(\frac{a^2 - pb^2}{a^2 - pb^2}, \frac{ab - ab}{a^2 - pb^2} \right) = (1, 0)$$

   since $a^2 = pb^2$ if and only if $a = \sqrt{p}b$ and hence $(a, b) = (0, 0)$. Distributivity is equally trivial:

$$\begin{aligned}
(a, b)((c, d) + (e, f)) &= (a, b)(c + e, d + f) \\
&= (ac + ae + pbd + pbf, ad + af + bc + be) \\
&= (ac + pbd, ad + bc) + (ae + pbf, af + be) \\
&= (a, b)(c, d) + (a, b)(e, f)
\end{aligned}$$

   Hence $\mathbb{Q}(\sqrt{p})$ is a field. Now let $f : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{q})$ be an isomorphism of fields where p, q are any two primes. From the additive and multiplicative properties of f is is fairly obvious that

$$f(m, n) = (m, 0)f(1, 0) + (n, 0)f(0, 1)$$

   where $m, n \in \mathbb{Q}$. $f(1, 0) = (1, 0)$ from the fact that this is an isomorphism. All that is left is to determine the value of $f(0, 1)$. Note that $f(0, 1)^2 = f(p, 0) = (p, 0)$. Hence we must find an $(a, b) \in \mathbb{Q}(\sqrt{q})$ such that $(a, b)^2 = (p, 0)$. But $(a, b)^2 = (a^2 + qb^2, 2ab)$. If this equals $(p, 0)$ then either $a = 0$ or $b = 0$. If $b = 0$ then $a^2 = p$ and hence a is not rational, so assume $a = 0$. Then we must find a rational $b = m/n$ in lowest terms such that $pn^2 = qm^2$. If $p = q$ then clearly $m = n = 1$, so assume $p \neq q$. Then $p \mid m^2$ and hence $p \mid m$, so that $m = kp$ and $n^2 = qpk^2$. But then $p \mid n^2$ and $p \mid n$, so m/n is not in lowest terms. Hence there is no such $m/n \in \mathbb{Q}$ and $p = q$. That is, $\mathbb{Q}(\sqrt{p}) \cong \mathbb{Q}(\sqrt{q})$ for p, q primes if and only if $p = q$.

4. *Let A be a commutative ring and $R = A[U]$. Show that if $f, g : R \to B$ are ring homomorphisms such that $f(x) = g(x)$ for all $x \in A \cup U$ then $f \equiv g$.*

   Define $Z = \{x \in C \mid f(x) = g(x)\}$, where $A \subset C$, and $U \subset C$ for some ring C. Then for all $x, y \in Z$, $f(x - y) = f(x) - f(y) = g(x) - g(y) = g(x - y)$ and $f(xy) = f(x)f(y) = g(x)g(y) = g(xy)$. Associativity and commutativity is inherited in the same way from R and B, and therefore Z is a subring of C. Since f and g agree on $A \cup U$, $A \cup U \subset Z$. Moreover, since $A[U]$ is by definition the smallest subring of C containing $A \cup U$, it follows that $A[U] \subset Z$, and hence $f(x) = g(x)$ for all $x \in R$.

5. *Find all the roots of $x^3 - x$ in $\mathbb{Z}_6[x]$.*

   $x^3 - x = x(x^2 - 1)$, so that either if $x^3 - x = 0$, $x = 0$, x is its own inverse, or x is a zero divisor. Clearly $x = 0$ and $x = 1$ are roots. $x = 5$ is a root since $5^1 - 1 = 24 \equiv 0 \mod 6$. $x = 2$ is a root since $2(2^2 - 1) = 6 \equiv 0 \mod 6$. $x = 3$ is a root since $3(3^2 - 1) = 24 \equiv 0 \mod 4$. $x = 4$ is a root since $4(4^2 - 1) = 60 \equiv 0 \mod 6$. So every element of $\mathbb{Z}_6$ is a root of this polynomial.

6. *Let F be a finite field. Show that* $\operatorname{char} F$ *is prime and that* $\prod_{a \in F^\times} a = -1$. *Deduce from this Wilson's Theorem:* $(p-1)! \equiv -1 \mod p$ *where p is prime.*

   The characteristic of a field F is the smallest positive integer p such that

   $$\underbrace{1 + 1 + \cdots + 1}_{p\ times}$$

   or 0 is there is no such integer. If p is composite then $p = nk$ for some n, k nonzero and less than p. But then

   $$\underbrace{1 + 1 + \cdots + 1}_{nk\ times} = \underbrace{(1 + 1 + \cdots + 1)}_{n\ times}\underbrace{(1 + 1 + \cdots + 1)}_{k\ times} = 0$$

   Since F is a field this means that one of $\underbrace{1 + 1 + \cdots + 1}_{n\ times}$ or $\underbrace{1 + 1 + \cdots + 1}_{k\ times}$ is zero, and hence that p is not minimal. Therefore, if p is minimal, p must be prime.

   Now let $|F| = q < \infty$ so that $|F^\times| = q - 1$. Assume that $q > 2$ since for $q = 2$ then result is trivial: $1 = -1$ and 1 is the only unit. Consider $a \in F^\times$ such that $a^2 = 1$, then $a^1 - 1 = (a - 1)(a + 1) = 0$ and hence $a = \pm 1$. Since a is a unit if and only if a^{-1} is a unit, $q - 1$ is always even. We can therefore pair each unit with its inverse, and, since -1 is always a unit, it follows that for $F^\times = \{a_1, \ldots, a_{q-1}\}$, letting $a_1 = 1$ and $a_2 = -1$,

   $$a_1 a_2 \cdots a_{q-1} = 1 \cdot -1 \cdot (a_3 a_3^{-1}) \cdots (a_{q-1} a_{q-1}^{-1}) = -1$$

   If $F = \mathbb{Z}/p\mathbb{Z}$ where p is prime, then F is a finite field of order p and the k such that $1 \le k \le p - 1$ are precisely the units of F. Therefore, by above, $(p-1)! \equiv -1 \mod p$.

7. *Let $f : \mathbb{Z}[x] \to \mathbb{C}$ be the ring homomorphism defined by $f(x) = i$ and $f(n) = n$ for $n \in \mathbb{Z}$. Show that* $\ker f = \{g \cdot (x^2 + 1) \mid g \in \mathbb{Z}[x]\}$ *and that this is the ideal generated by $x^2 + 1$ in $\mathbb{Z}[x]$.*

   f is defined by

   $$f\left(\sum a_k x^k\right) = \sum a_k i^k$$

   where $a_k \in \mathbb{Z}$. So that if $\sum a_k i^k = 0$, i is a root of the polynomial $\sum a_k x^k$. There exist polynomials q and r such that for any $p \in \ker f$, $p(x) = q(x)(x^2 + 1) + r(x)$. But as $p(i) = 0$, $r = 0$, and hence $p(x) = q(x)(x^2 + 1)$ for some polynomial $q \in \mathbb{Z}[x]$. So $\ker f \subset (x^2 + 1)$. Since $f(x^2 + 1) = 0$, $(x^2 + 1) \subset \ker f$, and therefore $\ker f = (x^2 + 1)$, the ideal generated by $x^2 + 1$.