NAP PRELIMINARY PROBLEM SET

ROGER AND SYLVIA WIEGAND

These problems were assigned during the first class, on 8 May, 2016. Solutions were turned in on 10 May. Roger and Sylvia will make comments on papers and return them to students on 11 May.

1. (This problem reconciles Milne's definition of "integral domain" with the usual definition.) Let R be a commutative ring with $1 \neq 0$. Prove that these two conditions are equivalent:

(a) For all $x, y, z \in R$ with $x \neq 0$, $xy = xz \implies y = z$.
(b) For all $x, y \in R \setminus \{0\}$, $xy \neq 0$.

Solution: First observe that $x \cdot 0 = 0$ for all $x \in R$. To see this, we have $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Adding $-x \cdot 0$ to both sides, we get $0 = x \cdot 0$.

Now assume (a) holds. Suppose, by way of contradicton, that $x \neq 0$ and $y \neq 0$, but $xy = 0$. Then $xy = x \cdot 0$ by the observation above. By (a), we have $y = 0$, contradiction. $\therefore$ (b) holds.

If (b) holds and $xy = xz$ with $x \neq 0$, we have $x(y - z) = xy = xz = 0$, whence $y - z = 0$, that is, $y = z$. $\therefore$ (a) holds.

$\therefore$ (a) $\iff$ (b). □

2. Let p be a prime number and n a positive integer. Prove that

$$p \;\Big|\; \binom{p^n}{\ell} \qquad \text{for } 0 < \ell < p^n\,.$$

Solution: A direct argument is certainly possible, but it's a little bit messy. Let's try another approach. In view of the binomial theorem, the assertion is equivalent to the following assertion about the polynomial ring $\mathbb{F}_p[X]$:

$$(1 + X)^{p^n} = 1 + x^{p^n} \qquad \text{for every } n \geq 1\,.$$

We'll prove this by induction on n, starting with the case $n = 1$. This case is, of course, equivalent to the case $n = 1$ in the original assertion, so we must show that

$$p \;\Big|\; \binom{p}{\ell} \qquad \text{for } 0 < \ell < p\,.$$

Put $N = \binom{p}{\ell} = \frac{p!}{p!(p-\ell)!}$. Then $p! = \ell!(p - \ell)!N$, and hence

$$p \mid \ell!(p - \ell)!N$$

$\therefore$ the case $n = 1$ holds.

For the inductive step, assume that $n \geq 1$ and that $(1 + X)^{p^n} = 1 + X^{p^n}$. Then $(1 + X)^{p^{n+1}} = ((1 + X)^{p^n})^p = (1 + X^{p^n})^p = 1 + (X^{p_n})^p = 1 + X^{p+1}$. (The second equality if from the inductive hypothesis, and the third equality is obtained by substituting X^{p^n} for the indeterminate X in the case $n = 1$.) □

3. Let a and b be elements of an integral domain R. Prove that $(a) = (b)$ if and only if $a \sim b$. (Recall that $\sim$ is the equivalence relation defined by $a \sim b$ if and only if there is a unit u of R such that $b = ua$. (Note: The conditions are not equivalent for arbitrary commutative rings, though it's not particularly easy to find counterexamples.)

Date: 11 May, 2016.

Solution: Assume that $(a) = (b)$. Then there exist $r, s \in R$ such that $b = ra$ and $a = sb$. If $a = 0$, the first equation forces $b = 0$ (by the observation in the solution of the first problem), so $a \sim b$. Suppose now that $a \neq 0$. We have $1a = a = rsa$, and therefore $1 = rs$ (by Milne's definition of "integral domain". Therefore r is a unit, so $a \sim b$.

For the converse, assume $a \sim b$, say, $b = ua$, where u is a unit. The equation says that $b \in (a)$, and hence $(b) \subseteq (a)$. Similarly, the equation $a = u^{-1}b$ shows that $(a) \subseteq (b)$. Therefore $(a) = (b)$. □