Math 153: HW Hints, Part II

Rich Schwartz

November 18, 2009

3.2.4 First $-x = (-x)(-x) = x^2 = x$. Second

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Using cancellation for the group, we get $ab = -ba = ba$.

3.2.6 Hint: The key point is that the same number works for all nonzero elements. Let's show that 6 cannot be the characteristic. Suppose that we have $a + a + a + a + a + a = 0$. Let $b = a + a$. Then $b \neq 0$ because 2 is less than the characteristic. But then $b + b + b = 0$, contradicting the fact that 3 is less than the characteristic.

3.2.7 The ring of polynomials over $\boldsymbol{Z}/2$ has characteristic 2.

3.2.10: Suppose R is an integral domain. If $ab = ac$ then $a(b - c) = 0$. Since $a \in R$ is nonzero, we have $b - c = 0$. Hence $b = c$. On the other hand, suppose that R is not an integral domain. then $ab = 0$ for some nonzero a, b. But then $ab = a0$ but $b \neq 0$. Hence, the cancellation property fails if R is not an integral domain.

3.4.3: Here's the easiest proof: The only ideals in a field are 0 and the whole field. So, the kernel of the homomorphism is either 0, or the whole field.

3.4.6: You just have to check closure under additivity, closure under (additive) inverses, and the absorber property. For the first property:

$$\sum a_i u_i v_i + \sum b_j u_j v_j = \sum (a_i + b_i) u_u v_i \in UV.$$

Here each a and each b is either 0 or 1. In case both a_i and b_i are 1, the expression $2u_iv_i$ means $u_iv_i + u_iv_i$. Here is the inverse property:

$$-\sum u_iv_i = \sum(-u_i)v_i \in UV$$

The absorber property is similar.

3.4.9: We need to make the same checks as the previous problem. For closure under addition,

$$(r_1 + r_2)u = r_1u + r_2u = 0 + 0 = 0.$$

For closure under inverses,

$$(-r)u = -ru = 0.$$

For the absorber property let $s \in R$ and $r \in r(U)$. Then

$$(sr)u = s(ru) = s0 = 0; \qquad (rs)u = r(su) = ru' = 0.$$

Here $u' \in U$ because U is an ideal.

3.4.12: Let I be an ideal in this ring. It suffices to prove that the identity matrix lies in I. Let $A \in I$ be some element. Multiplying on one side by elementary matrices (remember linear algebra) effects row reduction on A and keeps the result in I. So, I contains the row reduction B of A. Either B is the identity or one nonzero element. Say

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

In this case, one can permute the rows and columns of B by multplying on the left and right by permutation matrices to get $C \in I$, where

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then $B + C \in I$, and $B + C$ is the identity.

3.4.20: Every $r' \in R'$ has the form $\phi(r)$. So $\phi(1)r' = \phi(1r) = \phi(r) = r'$. Same with multiplication on the other side. So, $\phi(1)$ is the 1.

3.4.21: Let $r' \in R'$ be arbitrary.

$$r'\phi(1) = r'\phi(1 \times 1) = r'\phi(1)\phi(1).$$

We have cancellation in an integral domain, so

$$r' = r'\phi(1).$$

That does it.

3.5.1: We just have to show the existence of inverses. Suppose $a \in R$ is nonzero. Consider the right ideal aR. This is a nonzero ideal, so $1 \in aR$. This means that $ar = 1$ for some r. Applying the same argument for r, we see that $rb = 1$ for some b. But

$$b = arb = a.$$

So $ar = ra = 1$.

3.5.3: This is kind of tedious. Construct a homomorphism ϕ from J (the integers) into J_p. The hom. is just reduction mod p. Then check that the kernel of ϕ is exactly Jp.

3.6.4: We have inclusion $i : D \to K$. Define $\phi : D \to K$ by the map

$$\phi([a, b]) = i(a)(i(b)^{-1}).$$

Now just check that ϕ is well defined, and an isomomorphism.

3.6.6: This is just like what is done in the chapter for the field of fractions.

3.7.2: Suppose a and b are both greatest common divisors of c and d. Since a is a GCD, and b divides both c and d (because b is also a GCD) we have $b|a$ by definition of GCD. But $a|b$ as well. So $a = ub = (uv)a = 1a$. This means that $uv = 1$ and u, v are units. So a and b are associates.

3.7.3: If a is a unit then $ab = 1$ for some b. Then $d(a) \leq d(ab) = d(1)$. Also $d(1) \leq d(1a) = d(a)$. Combining these gives $d(1) = d(a)$. Conversely, if

$d(1) = d(a)$ then a is an element of the ideal $R = R1$ for which d is minimal. The then $R = Ra$. So, $1 = ab$ for some b. This does it.

3.7.6: The associative law comes from the definition of a ring. 1 is a unit, and hence serves as the identity. If u and v are units then we have $uu' = 1$ and $vv' = 1$. So $(uv)(u'v') = (uu')(vv') = 1$. So, we have closure under the group law. Finally if u is a unit then $uv = 1$ for some v. But then v is a unit, and also the inverse of u in the group.

3.8.2: All units have the same d value, and $d(1) = 1$.

3.8.3a: These elements are associates, because $-4 + 3i = i(3 + 4i)$. So, they each divide each other. So either one is a GCD for the pair.

3.8.4: Let p be prime congruent to 3 mod 4. In class we showed that $p = a^2 + b^2$ is impossible, by reducing mod 4. So, p is prime in $\boldsymbol{Z}[i]$. If $x^2 + 1 = 0$ has a solution mod p. Then we have $cp = (x + i)(x - i)$ in $\boldsymbol{Z}[i]$. But, since p is prime, we have $p|(x + i)$ or $p|(x - i)$. Either case is a contradiction.

3.8.6: Consider the number $N = 4p_1...p_n + 3$, where $p_1, ..., p_n$ is supposedly the complete list of primes congruent to 3 mod 4. None of these primes divides N. Factor N into primes and note that one of the primes on the list must be congruent to 3 mod 4 because N is congruent to 3 mod 4. This prime is a new prime congruent to 3 mod 4.