

Homework # 3, Section 6.3

Deep Creek Hot Springs

May 8, 2009



(no, those aren't Corey's feet, and he didn't take this picture. Although, he makes several trips there a year)

Section 6.3: 3, 4, 8, 11, 16, 19, 21, 29–31, 33–35, 39, 40. Why did I both assign so many questions, and then agree to type out solutions to said questions? Okay, here we go:

3. The only units are ± 1 and $\pm i$. Any other element $a + bi$ with inverse $c + di$ would satisfy

$$(ac - bd) + (ad + bc)i = 1 \iff ac - bd = 1, ad + bc = 0.$$

This occurs precisely when the following matrix equation is solved:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Or, namely, that $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ has an inverse, which would only be the case when its determinant, $a^2 + b^2$ is a unit. As a positive number, that would only be the case when $a^2 + b^2 = 1$, which immediately implies exactly one of a or b is 0, and the other is ± 1 .

4. The units are $(\pm 1, \pm 1)$, since both entries must be units.

8. I feel as though we did this one in class pretty thoroughly, would anyone mind if I didn't type it out?

11. Let c and d be multiplicative inverses of a . Notice that we can immediately conclude $a \neq 0$, and that a , as a unit, is *not* a zero divisor. Thus, by definition, $ac = ad = 1_R$, and

subtracting, we get $ac - ad = a(c - d) = 0$. Since $a \neq 0$, and a is not a zero divisor, we conclude that $c - d = 0$, and thus $c = d$.

16. The ring $\mathbb{Z}[i]$ is not a field, we noted that there aren't enough units in problem 3.

19. $\mathbb{Q}(\sqrt{3})$ IS a field, in fact, a subfield of \mathbb{R} . We apply the subfield test to show this. $\mathbb{Q}(\sqrt{3})$ is a nonempty subset of the real numbers, and we note that for $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, we have

$$(a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

We compute $(c + d\sqrt{3})^{-1} = \frac{1}{c^2 - 3d^2}(c - d\sqrt{3})$, and this fact can be checked directly, or by rationalizing the denominator of $\frac{1}{c + d\sqrt{3}}$. Notice the denominator is never 0 for any rational numbers c and d , since this would imply that $(c/d)^2 = 3$, and thus after division of two fractions of integers, yielding another fraction of integers, that $\sqrt{3}$ is rational, which is obviously false. Finally, we check

$$\begin{aligned} (a + b\sqrt{3})(c + d\sqrt{3})^{-1} &= \frac{1}{c^2 - 3d^2}(a + b\sqrt{3})(c - d\sqrt{3}) \\ &= \frac{1}{c^2 - 3d^2}((ac - bd) + (bc - ad)\sqrt{3}) \in \mathbb{Q}(\sqrt{3}). \end{aligned}$$

21. \mathbb{H} isn't commutative, and thus, not a field.

29. $\text{Char}\mathbb{Z}_3[i] = 3$.

30. $\text{Char}\mathbb{Z}_2 \times \mathbb{Q} \times \mathbb{Z}_3 = 0$, since one checks the (group theoretic) order of the unit $(1, 1, 1)$ as being infinite.

31. It is an elementary fact that if p is prime, then $\binom{p}{k}$ is divisible by p for all $k = 1, \dots, p - 1$, and of course, $\binom{p}{p} = \binom{p}{0} = 1$. Thus for every $k = 1, \dots, p - 1$, we have $\binom{p}{k} = 0 \pmod{p}$, and thus, in a field F with characteristic p , that $\binom{p}{k} = p \cdot a = 0$ for some $a \in F$. Then by the binomial theorem, we have

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + b^p.$$

33. From group theory, we have, for a finite group G and any element $g \in G$, that $g^{|G|} = e$, the identity. We apply this result to the group of units $U(F)$ of F . Since F has q elements, and every nonzero element is a unit since F is a field, we have $|U(F)| = q - 1$, and as a result, for any $0 \neq a \in F$, that $a^{q-1} = 1_F$. Multiplying by a , we have $a^q = a$. For the case $a = 0$, the result holds as well.

34. (a) One considers the elements $\omega_k - e^{2\pi ik/p} \in \mathbb{C}$, and sees that these are distinct, and each solve $x^p - 1 = 0$ in \mathbb{C} .

(b) Suppose that p is an odd prime. Then using problem 31,

$$\begin{aligned} x^p - 1 &= x^p + (-1)^p \\ &= (x + (-1))^p \\ &= (x - 1)(x - 1)^{p-1}. \end{aligned}$$

Since F is a field, it is an integral domain. Thus if x is a solution to $x^p - 1 = (x - 1)(x - 1)^{p-1} = 0$, then either $x - 1 = 0$ or $(x - 1)^{p-1} = 0$, and in either case we will eventually conclude that $x - 1 = 0$, or that $x = 1$, and thus there is only one solution to this equation.

35. I feel as though we also covered this one in detail in class, and so I'll not type it here.

39. Suppose R is an integral domain, $a \in R$, and that $a^2 = a$. Then $a^2 - a = a(a - 1) = 0$, which implies $a = 0$ or $a - 1 = 0$, or that $a = 1$.

40. The idempotents of \mathbb{Z}_6 are 0,1,3,4, and the idempotents of \mathbb{Z}_12 are 0,1,4,9. The element $(a, b)^2 = (a^2, b^2) = (a, b)$ if and only if $a^2 = a$ and $b^2 = b$. Hence the idempotents of the cross product are the cross product of the idempotents.