

## Page 377

7. Assume  $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ . If  $\sqrt{a}$  and  $\sqrt{b}$  are both rational then choose  $c = \frac{\sqrt{a}}{\sqrt{b}}$ . If exactly one is rational the two fields are clearly not equal, one is  $\mathbb{Q}$ , the other is strictly larger. Thus assume both  $\sqrt{a}$  and  $\sqrt{b}$  are irrational. We have:

$$\sqrt{a} = m + n\sqrt{b}$$

for  $m, n \in \mathbb{Q}$  where  $n \neq 0$  since  $\sqrt{a}$  is irrational. Squaring this gives

$$a = m^2 + 2mn\sqrt{b} + n^2b.$$

If  $m \neq 0$  then we can solve this equation for  $\sqrt{b}$  and conclude  $\sqrt{b}$  is rational, a contradiction. Thus  $m = 0$  so  $\sqrt{a} = n\sqrt{b}$  so  $a = n^2b$  as desired.

Conversely if  $a = bc^2$  then  $\sqrt{a} = c\sqrt{b}$  and it is clear that  $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ .

9. We have  $F \subseteq F(a) \subseteq E$ . If both containments are proper then Thm 21.5 implies  $[E : F]$  is not prime. So either  $F = F(a)$  or  $F(a) = E$ .

19. See back.

## Page 387

3.  $K$  is a finite field so  $K^*$  is cyclic by Thm 22.2. Suppose  $K^* = \langle a \rangle$ . Then clearly  $K = F(a)$ .

7. Notice that  $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$  and  $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$  by the freshman binomial theorem. Thus  $\phi$  is a ring homomorphism. Since we are over a field, the kernel is clearly 0, and thus  $\phi$  is 1-1. However the field is finite, so  $\phi$  is also onto, thus a field automorphism. By Thm 22.2 we know  $GF(p^n)^*$  is a cyclic group of order  $p^n - 1$ , say it is generated by  $\alpha$ . For any  $a$  we have  $a^{p^n - 1} = 1$ , i.e.  $a^{p^n} = a$ , i.e.  $\phi^n(a) = a$ . (because we have raised an element of a group to the order of the group power) Thus  $\phi^n$  is the identity map. Now we must show no smaller power of  $\phi$  is the identity map. However since  $\alpha$  generates the cyclic group, the smallest power of  $\alpha$  which is 1 is  $p^n - 1$ . Thus for  $m < n$  we have  $\phi^m(\alpha) \neq \alpha$ , so  $\phi$  has order  $n$ .

22. These lattices should be identical to the subgroup lattices for cyclic groups of order 18 and 30 respectively.

29. We know  $\alpha^{124} = 1$ . There are at most two roots to the polynomial  $x^2 - 1 = 0$ , thus these are  $\pm 1$ . (Notice  $1 \neq -1$  since the characteristic is not 2) But  $\alpha^{62}$  is a root. It can't equal 1 since  $\alpha$  generates the cyclic group of order 124. Thus  $\alpha^{62} = -1$ .

## Page 395

2. One can easily draw the triangle with sides 1 and  $a$  and then extend the base to length  $b$ . Then use the fact that given a point and a line we can draw a parallel line through the point to complete the diagram. Finally using similar triangles notice that the longest side of the big triangle has length  $ab$ .

4. One can construct the triangle shown in the same way as in 2. Then use similar triangles to observe that the base of the smaller triangle has length  $a/b$ .

6. This was discussed in class. One only needs to know that we can construct perpendicular lines.

**Page 560**

5. Suppose  $a, b \in E_H$  so  $\phi(a) = a, \phi(b) = b$  for all  $\phi \in H$ . Choose  $\phi \in H$ . Then  $\phi(a + b) = \phi(a) + \phi(b) = a + b$  so  $a + b \in E_H$ . Similarly for  $a/b$  and  $ab$ , so  $E_H$  is a subfield.

7. See back.