

HOMWORK SOLUTIONS MATH 432 ASSIGNMENT 9

Exercise 3.88

First there are p^3 monic cubic polynomials, so it suffices to count the reducible ones. We divide them into three groups: with 1,2,or 3 roots (counting multiples).

The number of cubic f with 3 roots is the number of methods choosing three numbers (counting multiples) in F_p . Not too difficult to find that equals $\binom{p}{3} + 2\binom{p}{2} + \binom{p}{1} = (p^3 + 3p^2 + 2p)/6$.

No cubic polynomial has exactly two roots. (Why?)

If f has exactly one root r , then it is of form $(x - r)g(x)$ where g is a monic irreducible quadratic polynomial. With similar discussion we know there are $p^2 - (\binom{p}{2} + \binom{p}{1}) = (p^2 - p)/2$ of them. So we have $p(p^2 - p)/2$ such cubic ones.

So finally the number of monic irreducible cubic polynomials is $p^3 - (p^3 + 3p^2 + 2p)/6 - p(p^2 - p)/2 = (p^3 - p)/3$.

Exercise 3.89

We can use the similar (but more complicated) argument as above, note that page 286 gives us the number of monic irreducible polynomials up to degree 4. Final answer 6.

Or since only two elements are in the base field, you can easily rule out those polynomials with 0 or 1 as roots. That will left you 8 possible ones. Two of them are products of irreducible quadratics and irreducible cubics and by the table in page 286 these are the only possible reducible ones in the remaining 8.

Exercise 3.93

We know that there is a unique constant in each equivalence class in $R[x]/(x)$, so define a map from $R[x]/(x)$ to R by mapping each equivalence class to the unique constant in it. It is not difficult to show that this is a homomorphism and bijection. Or try to use Isomorphism Theorem to get the result, by $\phi : f \mapsto f(0)$.

Exercise 3.100

(i) $x^4 + 1 = (x^2 + 1)^2$

(ii) Direct from the equality.

(iii) If $b^2 = -1$, then $x^4 + 1 = (x^2 + b)(x^2 - b)$; if $a^2 = \pm 2$, then $x^4 + 1 = (x^2 + ax \pm 1)(x^2 - ax \pm 1)$.

(iv) By Lemma 3.82 and Exercise 3.99.

Proof of 3.99:

We first prove that, for any group G , if $|G|$ is odd, then every element has a square root. Let $f : G \rightarrow G$ be the squaring map. If it is not bijective (injective) then there is g which is the square of x and y , i.e. $g = x^2 = y^2$. Then the subgroup generated by x or that generated by y must have even number of elements (this is not easy, but please try to do it yourself).

An easier proof is that, since every element g is of odd order, we know $g^{2k+1} = 1$, so $g^{sk+2} = g$, i.e. g^{k+1} is the square root of g . [Extra Credit to David Pinney for this simple proof.]

Then we see that F_p^\times is an abelian group of order $4k + 2$, if $p \equiv 3 \pmod{4}$. And $[p - 1] = [-1]$ generates a subgroup of order 2. Now take $H = F_p^\times / \langle -1 \rangle$, a quotient group of order $m = 2k + 1$. Notice that $\{[2], [-2]\} = [[2]] \in H$ has a square root in H , namely $[[m]]^2 = [[2]]$, then easy to see either $[2]$ or $[-2]$ is the square of $[m]$ in F_p^\times .