

2022 classes are filling fast. Reserve your spot today!

Group Theory (2900)

Justin Stevens

Sunday

Sep 26, 2021 - Jan 23, 2022

7:30 - 9:30 PM ET (4:30 - 6:30 PM PT)

Homework

Week: 1 2 3 4 5 6 7 8 9 10 11 **12** 13 14

Homework: Week 12

You have completed 11 of 11 challenge problems.

You did not submit a writing problem response.

Past Due Jan 17.

[Request Extension](#)

Readings

Week 12: Chapter 14

Week 13: Chapter 16

Week 12 Transcript: [Sun, Jan 9](#)

Challenge Problems

Problem 1 – Correct! – Score: 1 / 7 (39339)

[Report Error](#)

Problem:

For what monic polynomial f is $\mathbb{Q}[\omega] \cong \mathbb{Q}[x]/(f)$, if ω is a primitive 6th root of unity? (This means the order of ω is 6 in the multiplicative group.) Write your answer as a polynomial in standard form.

Solution:

While we have $\omega^6 = 1$, we cannot simply take $f(x) = x^6 - 1$, since this polynomial is reducible, and thus quotienting by it will not produce a field. We thus try to factor f into irreducible factors, to see which one ω is a root of. By applying the difference of squares and cubes and sum of cubes factorizations, we find

$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$. The first three factors correspond to the roots $x = 1$, $x = e^{\pm 2\pi i/3}$, and $x = -1$. The last factor is thus the f we're looking for.

Indeed, $x^2 - x + 1$ has the primitive sixth roots of unity as roots, and it is irreducible over \mathbb{Q} , simply because it does not have rational roots.

Hint(s): Didn't we have some assumptions on f in our construction of $k[x]/(f)$?

Your Response(s):

- ☐ $x^4 + 1$
- ☐ $x^4 + x^2 + 1$
- ☐ $x^4 + x^2 + 1$
- ☐ $x^6 - 1$
- ☐ $x^2 - x + 1$

Typesetting math: 100% – Correct! – Score: 5 / 7 (39641)

Problem:[Report Error](#)

For what monic polynomial f is $\mathbb{Q}[\omega] \cong \mathbb{Q}[x]/(f)$, if ω is a primitive 8th root of unity? (This means the order of ω is 8 in the multiplicative group.) Write your answer as a polynomial in standard form.

Solution:

The roots of $x^8 - 1$ that are not primitive eighth roots of unity are the fourth roots of unity, which satisfy $x^4 - 1 = 0$. That lets us find the desired f as the second factor in

$$x^8 - 1 = (x^4 - 1)(x^4 + 1).$$

Indeed, the roots of $x^4 + 1$ are exactly the fourth roots of -1 , including ω as desired.

And $x^4 + 1$ is irreducible. It has no linear factor since \mathbb{Q} contains no fourth roots of -1 . Thus if $x^4 + 1$ were reducible, we must have $x^4 + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$ for some $a, b \in \mathbb{Q}$. Since $x^4 + 1$ has no cubic term, we find $a + b = 0$. Since it has no quadratic term, we find $\pm 2 + ab = \pm 2 - a^2 = 0$. Thus $a = \pm\sqrt{2}$, which is not rational, and hence $x^4 + 1$ is irreducible. Thus, the desired polynomial is $x^4 + 1$.

Your Response(s):

☹ $x^6 + x^4 + x^2 + 1$

😊 $x^4 + 1$

Problem 2, Part (a) – Give Up – Score: 0 / 7 (39643)

Problem:[Report Error](#)

Let $k = \mathbb{Q}[\omega]$, where ω is a primitive 6th root of unity. Compute the reciprocal of $3 - 2\omega^2 + \omega^5$ in k . Enter your answers as integers; include any negatives in the numerator only.

Solution:

Since $\omega^5 = -\omega^2$, this is simply $3 - 3\omega^2$. Now we apply the conjugation trick, using that $\overline{\omega^2} = \omega^4 = -\omega$, so we can compute

$$(3 - 3\omega^2)(3 + 3\omega) = 9 + 9\omega - 9\omega^2 - 9\omega^3 = 27, \text{ where we use } \omega^3 = -1 \text{ and } \omega - \omega^2 = 2\operatorname{Re}(\omega) = 1.$$

$$\text{That means that } (3 - 3\omega^2)^{-1} = \frac{3 + 3\omega}{27} = \frac{1 + \omega}{9}.$$

Your Response(s):

☹ $(3 - 2\omega^2 + \omega^5)^{-1} = \frac{9 + -1\omega + 3\omega^2}{26}$

☹ Give Up

Problem 2, Part (b) – Give Up – Score: 0 / 7 (39645)

Problem:[Report Error](#)

Now let $k = \mathbb{Q}[\omega]$ where ω is a primitive eighth root of unity. Find the following reciprocal in k . Enter integers in the blanks below, using any non-positive entries only in the numerator.

Solution:

Here, we have the following automorphisms:

Typesetting math: 100%

☐ $\omega \mapsto \omega$, which sends $\omega^2 \mapsto \omega^6 = -\omega^2$. (Note ω^2 is i or $-i$.)

- $\omega \mapsto \omega^5$. Since $\omega^5 = -\omega$, this sends ω^2 to itself.
- $\omega \mapsto \omega^7 = -\omega^3$. This sends $\omega^2 \mapsto \omega^6 = -\omega^2$, again.

Thus to compute this reciprocal we have to first take the product

$$\begin{aligned} & (-2 + 3\omega)(-2 - 3\omega)(-2 + 3\omega^3)(-2 - 3\omega^3) \\ &= (4 - 9\omega^2)(4 + 9\omega^2) \\ &= 97. \end{aligned}$$

Then the reciprocal will come out to be

$$\begin{aligned} \frac{(-2 - 3\omega)(-2 + 3\omega^3)(-2 - 3\omega^3)}{97} &= \frac{(-2 - 3\omega)(4 + 9\omega^2)}{97} \\ &= \boxed{\frac{-8 - 12\omega - 18\omega^2 - 27\omega^3}{97}}. \end{aligned}$$

Your Response(s):

- ☹ $(-2 + 3\omega)^{-1} = \frac{2 + 0\omega + 0\omega^2 + 3\omega^3}{17}$
- ☹ $(-2 + 3\omega)^{-1} = \frac{-2 + 0\omega + 0\omega^2 + -3\omega^3}{1}$
- ☹ $(-2 + 3\omega)^{-1} = \frac{-4 + -6\omega + -6\omega^2 + -9\omega^3}{35}$
- ☹ Give Up

Problem 3 – Give Up – Score: 0 / 7 (39345)

Problem:

[Report Error](#)

Let ω be a primitive n th root of unity. How many automorphisms do the following extensions have? Recall that an automorphism of an extension K/k is an automorphism $\varphi : K \rightarrow K$ of the field K such that k is fixed by φ , that is, $\varphi(x) = x$ for every $x \in k$.

Solution:

$\mathbb{Q}[\sqrt[n]{2}]$ has no nontrivial automorphisms if n is odd and one if n is even, given in that case by $\sqrt[n]{2} \mapsto -\sqrt[n]{2}$. Indeed, any automorphism must send $\sqrt[n]{2}$ to another n th root of 2, but $\mathbb{Q}[\sqrt[n]{2}] \subset \mathbb{R}$, which contains only one n th root of 2, if n is odd, and two, if n is even.

In contrast, $\mathbb{Q}[\omega, \sqrt[n]{2}]$ contains all the n th roots of 2, namely $\omega^j \sqrt[n]{2}$ for all j . Furthermore, it coincides with $(\mathbb{Q}[\omega])[x]/(x^n - 2)$, so automorphisms are given by sending $\sqrt[n]{2}$ to any of the other n th roots of 2. The automorphism group is thus cyclic of order n , generated by $\sqrt[n]{2} \mapsto \omega \sqrt[n]{2}$.

Remark: This is a general phenomenon: extensions of fields that already contain the n th roots of unity by n th roots of some new number behave more naturally, in that they get all n automorphisms you might expect.

Your Response(s):

- ☹ Give Up

Typesetting math: 100%

Problem:

Report Error

Proof puzzle! Prove that any polynomial $f \in k[x]$ has at most $\deg(f)$ roots. Fill in the blanks below in the correct order.

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

$\frac{1}{1}$

??

Solution:

A sentence describing the general technique of the proof must come at its beginning.

We proceed by induction.

Ideally, the base case of an inductive proof is given first, though this is not a hard-and-fast rule.

For a base case, a polynomial of degree 0 has no roots, since such a polynomial is a nonzero constant.

Next, we make our inductive hypothesis.

Now suppose it is established that a polynomial of degree $m - 1$ has at most $m - 1$ roots.

Having done so, we proceed to the inductive step.

Let $f \in k[x]$ be a polynomial of degree m .

We intend to apply the inductive hypothesis to a root of f , but must first consider the case that this cannot be done at all:

If f has no roots, then it certainly has no more than m .

Otherwise, there is a root, and we can get into the core of the argument:

Otherwise, f has a root $a \in k$.

Here is the key step that lets us reduce to the inductive hypothesis:

By the division theorem, we know $f = (x - a)q + r$ for some $q, r \in k[x]$, with $\deg(r) < 1$.

And here is where we use the assumption that a is a root of f :

Since $f(a) = 0$ and $[(x - a)q](a) = 0$, this implies $r(a) = 0$, so $r = 0$.

Now we make explicit the upcoming application of the inductive hypothesis:

Therefore $f = (x - a)q$, where $\deg(q) = m - 1$.

But it cannot be applied until we know b is a root of q :

If $b \neq a \in k$ is another root of f , then $f(b) = (b - a)q(b) = 0$, and by the ZPP, $q(b) = 0$.

Typesetting math: 100%

Finally, the inductive hypothesis applies:

By the inductive hypothesis, there can be at most $m - 1$ possibilities for roots of f different from a .

And we wrap it up:

Thus f has at most m roots, as was to be shown.

Your Response(s):

☹ We proceed by induction., For a base case, a polynomial of degree 0 has no roots, since such a polynomial is a nonzero constant., Now suppose it is established that a polynomial of degree $m-1$ has at most $m-1$ roots., Let $f \in k[x]$ be a polynomial of degree m ., If f has no roots, then it certainly has no more than m ., By the division theorem, we know $f = (x-a)q + r$ for some $q, r \in k[x]$, with $\deg(r) < 1$., Since $f(a) = 0$ and $[(x-a)q](a) = 0$, this implies $r(a) = 0$, so $r = 0$., If $b \neq a \in k$ is another root of f , then $f(b) = (b-a)q(b) = 0$, and by the ZPP, $q(b) = 0$., Otherwise f has a root $a \in k$., By the inductive hypothesis, there can be at most $m-1$ possibilities for b ., Therefore $f = (x-a)q$, where $\deg(q) = m-1$., Thus f has at most m roots, as was to be shown.

☹ Let $f \in k[x]$ be a polynomial of degree m ., If f has no roots, then it certainly has no more than m ., We proceed by induction., For a base case, a polynomial of degree 0 has no roots, since such a polynomial is a nonzero constant., Now suppose it is established that a polynomial of degree $m-1$ has at most $m-1$ roots., By the division theorem, we know $f = (x-a)q + r$ for some $q, r \in k[x]$, with $\deg(r) < 1$., Since $f(a) = 0$ and $[(x-a)q](a) = 0$, this implies $r(a) = 0$, so $r = 0$., If $b \neq a \in k$ is another root of f , then $f(b) = (b-a)q(b) = 0$, and by the ZPP, $q(b) = 0$., Otherwise f has a root $a \in k$., By the inductive hypothesis, there can be at most $m-1$ possibilities for b ., Therefore $f = (x-a)q$, where $\deg(q) = m-1$., Thus f has at most m roots, as was to be shown.

☹ Let $f \in k[x]$ be a polynomial of degree m ., If f has no roots, then it certainly has no more than m ., We proceed by induction., For a base case, a polynomial of degree 0 has no roots, since such a polynomial is a nonzero constant., Now suppose it is established that a polynomial of degree $m-1$ has at most $m-1$ roots., By the division theorem, we know $f = (x-a)q + r$ for some $q, r \in k[x]$, with $\deg(r) < 1$., Since $f(a) = 0$ and $[(x-a)q](a) = 0$, this implies $r(a) = 0$, so $r = 0$., Otherwise f has a root $a \in k$., If $b \neq a \in k$ is another root of f , then $f(b) = (b-a)q(b) = 0$, and by the ZPP, $q(b) = 0$., By the inductive hypothesis, there can be at most $m-1$ possibilities for b ., Therefore $f = (x-a)q$, where $\deg(q) = m-1$., Thus f has at most m roots, as was to be shown.

☹ We proceed by induction., For a base case, a polynomial of degree 0 has no roots, since such a polynomial is a nonzero constant., Now suppose it is established that a polynomial of degree $m-1$ has at most $m-1$ roots., Let $f \in k[x]$ be a polynomial of degree m ., If f has no roots, then it certainly has no more than m ., By the division theorem, we know $f = (x-a)q + r$ for some $q, r \in k[x]$, with $\deg(r) < 1$., Since $f(a) = 0$ and $[(x-a)q](a) = 0$, this implies $r(a) = 0$, so $r = 0$., Otherwise f has a root $a \in k$., If $b \neq a \in k$ is another root of f , then $f(b) = (b-a)q(b) = 0$, and by the ZPP, $q(b) = 0$., By the inductive hypothesis, there can be at most $m-1$ possibilities for b ., Therefore $f = (x-a)q$, where $\deg(q) = m-1$., Thus f has at most m roots, as was to be shown.

☺ Give Up

Problem 4, Part (b) – Give Up – Score: 0 / 7 (39360)

Problem:

[Report Error](#)

Let $q = p^n$ for a prime p . Find a monic polynomial of degree q in the variable x for which every element of \mathbb{F}_q must be a root (assuming such a field exists.)

Solution:

The multiplicative group $\mathbb{F}_{p^n}^\times$ is of order $p^n - 1$, so by Lagrange's theorem, every order of an element of this group divides $p^n - 1$. Therefore, for every nonzero element x of \mathbb{F}_{p^n} , we must have $x^{p^n - 1} = 1$, the identity of $\mathbb{F}_{p^n}^\times$. In particular, $x^{p^n} = x$ if $x \in \mathbb{F}_{p^n}^\times$; of course, 0 is also a root of this polynomial. Therefore every element of \mathbb{F}_{p^n} is a root of

$$x^{p^n} - x.$$

Typesetting math: 100%

Note that this, together with the previous problem, shows that any field of order p^n consists of *all* the possible roots of $x^{p^n} - x$. This gives a rough idea of an approach to prove that \mathbb{F}_{p^n} always exists and is unique: explain how to build a field out of the roots of some polynomial in a unique way. Such a construction exists and is called the *splitting field* of the polynomial.

Your Response(s):

☹ Give Up

Problem 5, Part (a) – Give Up – Score: 0 / 7 (39342)

Problem:

[Report Error](#)

For the field $k = \mathbb{Q}[x]/(x^3 - 2)$, how many subfields $K \subseteq \mathbb{C}$ are isomorphic to k , and how many automorphisms does k have?

Solution:

In class it was established that homomorphisms $k \rightarrow \mathbb{C}$ are uniquely determined by a choice of cube root of 2 in \mathbb{C} . For any such cube root α , we thus have to see whether the subfield $K = \{s + t\alpha + r\alpha^2 \mid s, t, r \in \mathbb{Q}\}$ contains any other cube root of 2. If $\alpha \in \mathbb{R}$, then $K \subseteq \mathbb{R}$, and the other two cube roots of 2 are non-real, so they are not present. Conversely, if α is not real, then K does not contain the real cube root of 2, since then K would contain the whole subfield generated by the real cube root of 2, which is already isomorphic to k .

If now α is one of the non-real cube roots of 2, we must thus see whether the other non-real cube root, $\bar{\alpha}$, is in K . Without loss

of generality, we can consider $\alpha = \sqrt[3]{2}e^{2\pi i/3} = -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2}\sqrt{3}}{2}i$, so that

$\alpha^2 = \sqrt[3]{4}e^{4\pi i/3} = -\frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4}\sqrt{3}}{2}i$. Then we are asking whether we can solve

$$s + t\alpha + r\alpha^2 = \bar{\alpha} = -\frac{\sqrt[3]{2}}{2} - \frac{\sqrt[3]{2}\sqrt{3}}{2}i$$

for rationals s, t, r .

Equating real parts, this implies

$$s - t\frac{\sqrt[3]{2}}{2} - r\frac{\sqrt[3]{4}}{2} = -\frac{\sqrt[3]{2}}{2},$$

so we must have $s = r = 0$ and $t = 1$. Indeed, since $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ with a basis $1, \sqrt[3]{2}, \sqrt[3]{4}$, we know s, t, r are uniquely determined. But since $0 + 1 \cdot \alpha + 0 \cdot \alpha^2 = \alpha \neq \bar{\alpha}$, this shows $\bar{\alpha} \notin K$. Therefore there are 3 distinct subfields of \mathbb{C} isomorphic to k .

Turning to automorphisms, an automorphism of k must send x to another cube root of 2 in k , since it respects addition, multiplication, and 0. However, by the above arguments, there are no such other cube roots of 2 in k : if there were, then the embeddings of k in \mathbb{C} should also contain more than one cube root of 2, but we have established they do not. Thus k has only 1 automorphism.

Your Response(s):

☹ Give Up

Problem 5, Part (b) – Give Up – Score: 0 / 7 (39341)

Typesetting math: 100%


Problem:[Report Error](#)

For the field $k = \mathbb{Q}[i, \sqrt{2}] \cong \mathbb{Q}[x]/(x^4 - 2x^2 + 9)$ discussed in class, how many subfields $K \subseteq \mathbb{C}$ are isomorphic to $\mathbb{Q}[\sqrt{2}, i]$, and how many automorphisms does k have?

Solution:

If $\mathbb{Q}[\sqrt{2}, i] \rightarrow K$ is an isomorphism with a subfield of \mathbb{C} , then we know we must map $\sqrt{2}$ to $\pm\sqrt{2}$ and i to $\pm i$. All four of these options give the same image, so there is only such subfield. Meanwhile, there are automorphisms, generated by complex conjugation and by radical conjugation with respect to $\sqrt{2}$. (These two automorphisms generate a Klein 4-group, while since any automorphism must send $i + \sqrt{2}$ to another root of $x^2 - 2x^2 + 9$, there can be no more than 4.)

Your Response(s):

 Give Up

Problem 5, Part (c) – Give Up – Score: 0 / 7 (39343)

Problem:[Report Error](#)

For the field $k = \mathbb{Q}[x]/(x^4 - 3x^2 - 1)$, how many subfields $K \subseteq \mathbb{C}$ are isomorphic to k , and how many automorphisms does k have? Furthermore, what is the degree over \mathbb{Q} of the subfield $\ell \subseteq k$ formed by those elements of k fixed by every automorphism of k over \mathbb{Q} ?

Solution:

Using the quadratic formula, we find that $x^4 - 3x^2 - 1 = 0$ if and only if

$$x^2 = \frac{3}{2} \pm \frac{\sqrt{13}}{2}.$$

In other words, we can factor $x^4 - 3x^2 - 1$ over $\mathbb{Q}[\sqrt{13}]$ as

$$\left(x^2 - \left(\frac{3}{2} + \frac{\sqrt{13}}{2}\right)\right) \left(x^2 - \left(\frac{3}{2} - \frac{\sqrt{13}}{2}\right)\right), \text{ and over a further extension field as the product of the four}$$


terms $x \pm \sqrt{\frac{3}{2} \pm \frac{\sqrt{13}}{2}}$. Note that two of these roots are real and two are complex.

As established in class, we have four homomorphisms $k \rightarrow \mathbb{C}$, one for each of the four roots of $x^4 - 3x^2 - 1$ in \mathbb{C} found above. However, since $x^4 - 3x^2 - 1$ is an even function, if $K \subset \mathbb{C}$ contains some root α , then it also contains a second root, $-\alpha$. So there are at most two choices for K . But since the choice of K containing the two real roots contains no non-real numbers, we see there really are subfields of \mathbb{C} isomorphic to k .

Turning to automorphisms, we note that $x \mapsto -x$ is a nontrivial automorphism, since $-x$ is another root of $x^4 - 3x^2 - 1$. Since we have shown above that there are fields isomorphic to k containing precisely two roots of $x^4 - 3x^2 - 1$, and any automorphism of k must send x to another such root, we see this is the only nontrivial automorphism, and there are in total.

Finally, the subfield of k fixed by the automorphism $x \mapsto -x$ is visibly $\ell = \{a + bx^2\} \subseteq k$, a subset which is closed

Typesetting math: 100% since x^4 is in ℓ . We see ℓ is of degree over \mathbb{Q} .

Your Response(s):
 Give Up

Problem 6 – Completed – Score: 3 / 3 (39344)

Problem:[Report Error](#)

Formulate and prove a conjecture relating the number of automorphisms of $k = \mathbb{Q}[x]/(f)$ for an irreducible polynomial f , distinct subfields in \mathbb{C} isomorphic to k , and the degree of k over \mathbb{Q} .

Beast Problem! You can skip this without penalty.

Solution:

In each of the past three examples of extensions k/\mathbb{Q} , we found that $|\text{Aut}(k)| \cdot m = [k : \mathbb{Q}]$, where m is the number of distinct subfields of \mathbb{C} isomorphic to k . Let us prove this conjecture.

A key step is to identify $[k : \mathbb{Q}]$ with the number of homomorphisms $k \rightarrow \mathbb{C}$, which we know we can do since we proved in class that such an homomorphism is uniquely determined by sending x to some root of f in \mathbb{C} . Since f is irreducible, it lacks repeated roots, and so f has $\deg(f) = [k : \mathbb{Q}]$ roots in \mathbb{C} .

Next, we observe that the group $\text{Aut}(k)$ acts on the set $\text{Hom}(k, \mathbb{C})$ of homomorphisms $k \rightarrow \mathbb{C}$ by composition: $\psi \star \varphi = \varphi \circ \psi$. Note that we established in class that $|\text{Hom}(k, \mathbb{C})| = |\deg(f)|$, since there is one homomorphism for each root of f in \mathbb{C} .

We claim that the orbit of any $\varphi : k \rightarrow \mathbb{C}$ under this action is the set of all homomorphisms of k into \mathbb{C} whose image is $\varphi(k)$. Indeed, the image of $\varphi \circ \psi$ is certainly $\varphi(k)$ for any $\psi \in \text{Aut}(k)$, since ψ is a bijection. Conversely, if $\varphi_1, \varphi_2 : k \rightarrow \mathbb{C}$ are embeddings with the same image K , then restricting the codomain to K turns φ_1, φ_2 into isomorphisms $\chi_1, \chi_2 : k \cong K$; we can thus get an automorphism of k by $\psi = \chi_2^{-1} \circ \chi_1$, and we see that $\psi \star \varphi_2 = \varphi_1$, so that φ_1 and φ_2 are in the same $\text{Aut}(k)$ -orbit as desired.

Furthermore, this $\text{Aut}(k)$ action has trivial stabilizers, since any embedding of k in \mathbb{C} is injective and nontrivial automorphisms of k have some non-fixed points. Therefore, by the orbit-stabilizer theorem, each orbit in $\text{Hom}(k, \mathbb{C})$ has $|\text{Aut}(k)|$ elements. There are m orbits, and they partition $\text{Hom}(k, \mathbb{C})$, so the result is proven.

Hint(s): Once you have your conjecture made, try to make it an equation about a group action.

Your Response:

asdf

Problem 7 – Did Not Answer – Technical: 0 / 7 – Style: 0 / 1 (39338)

Problem:[Report Error](#)

Let p be a prime number. Show by counting appropriate elements of $\mathbb{F}_p[x]$ that there exist fields of order p^2 and p^3 for every prime p .

Solution:

We aim to construct \mathbb{F}_{p^2} and \mathbb{F}_{p^3} as $\mathbb{F}_p[x]/(f)$ for some $f \in \mathbb{F}_p[x]$. If $\deg(f) = n$, we have

$$\mathbb{F}_p[x]/(f) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{F}_p\},$$

so it follows that $|\mathbb{F}_p[x]/(f)| = p^n$. As we know, this quotient is a field if and only if f is irreducible. Therefore our task is to prove that there is some irreducible polynomial of degree 2 and of degree 3 in $\mathbb{F}_p[x]$.

Typesetting math: 100%

Now, if $f \in \mathbb{F}_p[x]$ is a reducible quadratic, then it must be a product of two linear factors. If f is monic, then those factors may be taken to be monic, in which case they are uniquely determined as $x - r$ and $x - s$, where $r, s \in \mathbb{F}_p$ are the roots of f . Therefore the number of reducible monic quadratics in $\mathbb{F}_p[x]$ is $p + \binom{p}{2}$: there are p quadratics $(x - r)^2$ with a repeated root, and $\binom{p}{2}$ with two distinct roots. We have

$$p + \binom{p}{2} = p + \frac{p(p-1)}{2} = \frac{2p + p^2 - p}{2} = \frac{p^2}{2} + \frac{p}{2}.$$

On the other hand, there are p^2 monic quadratics in $\mathbb{F}_p[x]$, since the linear and constant terms can be chosen freely. The difference $p^2 - \frac{p^2}{2} - \frac{p}{2}$ is $\frac{p^2}{2} - \frac{p}{2}$, a quadratic in p which is only negative between its roots $p = 0$ and $p = 1$. In particular, there are always a positive number of irreducible, monic quadratics in $\mathbb{F}_p[x]$.

Moving on to the cubic case, if $f \in \mathbb{F}_p[x]$ is cubic, monic, and reducible, then we may write f as $(x - r)g$, where g is an irreducible monic quadratic, or as a product of three monic linear terms. For the latter case, we have $\binom{p}{3}$ reducible monic cubics with three distinct roots, $p \cdot (p-1)$ reducible monic cubics of the form $(x - r)^2(x - s)$ with $r \neq s$, and p reducible monic cubics of the form $(x - r)^3$. In the former case $f = (x - r)g$, with g irreducible, we have p choices for r and, from the previous paragraph, $\frac{p^2 - p}{2}$ choices for g .

Altogether, we get

$$\begin{aligned} \binom{p}{3} + p(p-1) + p + \frac{p^3 - p^2}{2} &= \frac{p(p-1)(p-2) + 6p(p-1) + 6p + 3p^3 - 3p^2}{6} \\ &= \frac{p^3 - 3p^2 + 2p + 6p^2 - 6p + 6p + 3p^3 - 3p^2}{6} \\ &= \frac{4p^3 + 2p}{6} \end{aligned}$$

reducible monic cubics in $\mathbb{F}_p[x]$, as against p^3 monic cubics in total. Thus the number of irreducible monic cubics is (if nonnegative) $\frac{2p^3 - 2p}{6} = p \cdot \frac{p^2 - 1}{3}$.

Again this difference is positive for $p > 1$, so there must exist irreducible monic cubics for every p .

To sum up, we have shown that for every p , we have irreducible quadratics and cubics in $\mathbb{F}_p[x]$, which means we can form \mathbb{F}_{p^2} and \mathbb{F}_{p^3} via the construction $\mathbb{F}_p[x]/(f)$, where f is such a polynomial.

Hint(s): It simplifies the counting to focus on monics.
Have you tried complementary counting?

Your Response:

You did not answer this problem.

Copyright © AoPS Incorporated. This page is copyrighted material. You can view and print this page for your own use, but you cannot share the contents of this page with others.

© 2022 Art of Problem Solving

[About Us](#) • [Contact Us](#) • [Terms](#) • [Privacy](#)

Copyright © 2022 Art of Problem Solving