HOMEWORK-4

SIDDHANT CHAUDHARY
BMC201953

29. Artin Chapter 12: 3.4.

Solution. Let x, y, z, w be four variables, and consider the polynomial $xy - zw$ is an irreducible element of $\mathbb{C}[x, y, z, w]$. We know that $\mathbb{C}[x, y, z, w] \cong \mathbb{C}[y, z, w][x]$. Any non-trivial factorisation of $xy - zw$ in $\mathbb{C}[x, y, z, w]$ will give us a non-trivial factorisation in $\mathbb{C}[y, z, w][x]$, and so it is enough to just work in $\mathbb{C}[y, z, w][x]$.

As we saw in Lecture 7, the ring $\mathbb{C}[y, z, w]$ is a UFD. Let Fr be the fraction field of $\mathbb{C}[y, z, w]$. Consider the polynomial $xy - zw \in \mathbb{C}[y, z, w][x]$, and consider the prime $z \in \mathbb{C}[x, y, z, w]$. Clearly, z does not divide y, z divides zw and z^2 does not divide zw. So, by **Eisenstein's Criterion**, we see that the polynomial $xy - zw$ is irreducible over Fr$[x]$. However, the polynomial $xy - zw \in \mathbb{C}[y, z, w][x]$ is *primitive*, because the gcd of y, zw is clearly 1. So, by **Gauss' Lemma**, it follows that $xy - zw$ is irreducible over $\mathbb{C}[y, z, w][x]$, and hence it is irreducible over $\mathbb{C}[x, y, z, w]$. This completes the proof. ■

30. Artin Chapter 12: 4.5bc + 4.6 + 4.16.

Solution. **4.5 (b)** $8x^3 - 6x + 1$. Since this is a cubic polynomial, it is enough to check whether it has any roots in $\mathbb{Q}$, and to do so we can use the **Rational Root Theorem**. So, it p/q is any root of this polynomial (in lowest terms), then $p|1$ and $q|8$. So, the choices for p are ± 1 and the choices for q are $\pm 1, \pm 2, \pm 4$ and ± 8. By computation, it can be easily checked that none of these possibilities for p and q gives a root of $8x^3 - 6x + 1$. So, this polynomial is *irreducible* over $\mathbb{Q}[x]$.

4.5 (c) $x^3 + 6x^2 + 1$. Again, this is a cubic polynomial, and it is enough to check whether this polynomial has any roots in $\mathbb{Q}$, and we will again use the **Rational Root Theorem**. So, if p/q is a root of this polynomial (in lowest terms), then $p|1$ and $q|1$, and hence the only choices for p, q are ± 1. However, neither 1 or -1 is a root of this polynomial, and hence this polynomial is *irreducible* over $\mathbb{Q}[x]$.

4.6 Consider the polynomial x^5+5x+5. We will factor it into irreducible factors in $\mathbb{Q}[x]$ and $\mathbb{F}_2[x]$. First, consider the ring $\mathbb{Q}[x]$. We can apply **Eisenstein's Criterion** here with $p = 5$. Clearly, the leading coefficient is not divisible by 5, and every other coefficient is divisible by 5. Moreover, the constant term is not divisible by 25, and hence this polynomial is irreducible over $\mathbb{Q}[x]$. So, this polynomial *cannot* be factored non-trivially over $\mathbb{Q}[x]$.

Next, consider the ring $\mathbb{F}_2[x]$, and the polynomial becomes $x^5 + x + 1$. Suppose this polynomial was *reducible*. It is easy to see that it does not have a root over $\mathbb{F}_2$, and hence it must factor into a degree 2 irreducible factor and a degree 3

Date: December 2020.

irreducible factor over $\mathbb{F}_2[x]$. Now, the *only* irreducible factor of degree 2 in $\mathbb{F}_2[x]$ is x^2+x+1. By long division, we see that

$$x^5+x+1=(x^2+x+1)(x^3+x^2+1)$$

and clearly, x^3+x^2+1 is irreducible in $\mathbb{F}_2[x]$ because it does not have any root. So this is the required factorisation.

4.16 Consider the polynomial $p(x)=x^{14}+8x^{13}+3$ in $\mathbb{Q}[x]$. Using reduction modulo 3 as a guide, we will show that this polynomial is irreducible. Note that this polynomial is *primitive* over $\mathbb{Z}[x]$, and hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. Now, suppose $p(x)=g(x)h(x)$ for $g,h\in\mathbb{Z}[x]$, and without loss of generality we assume that both $g(x)$ and $h(x)$ are monic. Reducing mod 3, we have

$$\overline{p}(x)=x^{14}+2x^{13}=x^{13}(x+2)\quad\text{in } \mathbb{F}_3[x]$$

and so it follows that $\overline{g}(x)\overline{h}(x)=x^{13}(x+2)$ in $\mathbb{F}_3[x]$. Because $\mathbb{F}_3[x]$ is a UFD, factors are unique upto units, and hence we can assume that $\overline{g}(x)=x^k$ and $\overline{h}(x)=x^{13-k}(x+2)$, for some $0\le k\le 13$. Also, observe that either the constant term of g or the constant term of h is *not* divisible by 3 (because the constant term of $p(x)$ is 3), and hence either $\overline{g}(x)$ or $\overline{h}(x)$ has a non-zero constant term, i.e either $k=0$ or $k=13$.

Now if $k=13$, then we see that $\overline{g}(x)=x^{13}$ and $\overline{h}(x)=x+2$ in $\mathbb{F}_3[x]$. Now, because deg$(g)+$deg$(h)=14$ and deg$(\overline{h})=1$, we see that deg$(h)=1$. This implies that $p(x)$ has a linear factor in $\mathbb{Z}[x]$, i.e $p(x)$ has a root in $\mathbb{Q}$. But using the **Rational Root Theorem**, we see that the only possible rational roots of $p(x)$ are ±3, and clearly neither of these are roots of $p(x)$. So, this is a contradiction, and hence $k=13$ is not possible.

So, it must be true that $k=0$, and hence $\overline{h}(x)=x^{13}(x+2)$ in $\mathbb{F}_3[x]$. Again, we know that deg$(g)+$deg$(h)=14$ and because deg $\overline{h}=14$, we see that deg$(g)=0$, i.e $g(x)=1$. So, it follows that the polynomial $p(x)$ is irreducible in $\mathbb{Z}[x]$, and therefore in $\mathbb{Q}[x]$. This completes the proof. ■

31. Artin Chapter 15: 2.1.

***Solution*.** Let α be a complex root of the polynomial x^3-3x+4. We find an inverse of $\alpha^2+\alpha+1$ in $\mathbb{Q}(\alpha)$, i.e in the form $a+b\alpha+c\alpha^2$ with $a,b,c\in\mathbb{Q}$. Suppose

$$(a+b\alpha+c\alpha^2)(1+\alpha+\alpha^2)=1$$

Expanding, we get

$$c\alpha^4+(b+c)\alpha^3+(a+b+c)\alpha^2+(a+b)\alpha+a=1$$

Now, we use the relations $\alpha^3=3\alpha-4$ and $\alpha^4=3\alpha^2-4\alpha$ to get

$$3c\alpha^2-4c\alpha+(b+c)(3\alpha-4)+(a+b+c)\alpha^2+(a+b)\alpha+1=1$$

which implies

$$(a+b+4c)\alpha^2+(a+4b-c)\alpha+a-4b-4c=1$$

Now, we know that the elements $1, \alpha, \alpha^2$ form a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha)$, i.e these elements are linearly independent. So, we get that

$$a + b + 4c = 0$$
$$a + 4b - c = 0$$
$$a - 4b - 4c - 1 = 0$$

We can solve these equations to get that

$$(a, b, c) = \frac{1}{49}(17, -5, -3)$$

and this gives us the required element. ■

32. Artin Chapter 15: 2.3 (Hint: proposition 15.2.8).

Solution. We will use the hint here. Let $\beta = \omega\sqrt[3]{2}$ where $\omega = e^{2\pi i/3}$ and let $K = \mathbb{Q}(\beta)$. Observe that both β and $\sqrt[3]{2}$ are roots of the polynomial $x^3 - 2$ (as ω is a cube root of unity), which is irreducible over $\mathbb{Q}[x]$ by **Eisenstein's Criterion** with $p = 2$. So, it follows that this polynomial is the minimal polynomial of both β and $\sqrt[3]{2}$, i.e β and $\sqrt[3]{2}$ both have the same minimal polynomial over the field $\mathbb{Q}$. So by the Proposition in the given hint, we have

$$\mathbb{Q}(\beta) \cong \mathbb{Q}(\sqrt[3]{2})$$

via an isomorphism that sends β to $\sqrt[3]{2}$ and that restricts to the identity on $\mathbb{Q}$. Now, if the equation

$$x_1^2 + ... + x_k^2 = -1$$

has a solution in $\mathbb{Q}(\beta)$ then the same equation also has a solution in $\mathbb{Q}(\sqrt[3]{2})$, because any solution in $\mathbb{Q}(\beta)$ is mapped to a solution in $\mathbb{Q}(\sqrt[3]{2})$ via an isomorphism. Now, we see that

$$\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$$

and hence the equation *cannot* have any solution in $\mathbb{Q}(\sqrt[3]{2})$, because the sums of squares of arbitrary numbers in $\mathbb{R}$ cannot be negative. So, it follows that the equation has no solution in $\mathbb{Q}(\beta)$. ■

33. Artin Chapter 15: 3.2.

Solution. We show that the polynomial $f(x) = x^4 + 3x + 3$ is irreducible over the field $\mathbb{Q}(\sqrt[3]{2})$. First, observe that this polynomial is irreducible over $\mathbb{Q}$ by **Eisenstein's Criterion** with $p = 3$.

Let $K = \mathbb{Q}(\sqrt[3]{2})$. Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, we see that $[K : \mathbb{Q}] = 3$. Let $\alpha \in \mathbb{C}$ be any root of f, and consider the field $\mathbb{Q}(\alpha)$. Since f is irreducible in $\mathbb{Q}[x]$ and has α as a root, it follows that f is the minimal polynomial of α over $\mathbb{Q}$ and hence $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Now observe that $\mathbb{Q} \subset K \subset K(\alpha)$, and hence

$$[K(\alpha) : \mathbb{Q}] = [K(\alpha) : K][K : Q] = 3[K(\alpha) : K]$$

Also, we see that $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K(\alpha)$, and hence

$$[K(\alpha) : \mathbb{Q}] = [K(\alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4[K(\alpha) : \mathbb{Q}(\alpha)]$$

The above implies that $4|[K(\alpha) : \mathbb{Q}]$, and this implies that $4|[K(\alpha) : K]$. Because $f(x)$ is a polynomial in $K[x]$ and contains α as one of its roots, it follows that α is algebraic over K. Suppose g is the minimal polynomial of α over K. So, we see that deg$(g) = [K(\alpha) : K] = 4$. But since f already has degree 4, it follows that f *is* the minimal polynomial of α over K, i.e $f(x)$ is irreducible in $K[x]$. This completes the proof. ■

34. Artin Chapter 15: 7.4 (Count for general p and then substitute p = 3, 5. Gauss discovered a very nice formula for the number of irreducible polynomials of a given degree over a finite field. We will soon see all the ingredients necessary to prove this formula. This is standard, but here is a short friendly exposition:)

https://arxiv.org/pdf/1001.0409v6.pdf

Solution. First, we will count the number of irreducibles of degree 3 over $\mathbb{F}_p[x]$ for a prime p. To do this, we will first count the number of *reducibles*. Let $f(x) \in \mathbb{F}_p[x]$ be a reducible polynomial, i.e $f(x)$ factors non-trivially in $\mathbb{F}_p[x]$. So, $f(x)$ must have a linear factor, i.e $f(x)$ has a root in $\mathbb{F}_p$. Now, there are two cases.

(1) The quadratic factor of $f(x)$ is *irreducible*. So, in this case, we can write $f(x) = a(x-\alpha)(x^2+bx+c)$ for some $a \neq 0$, $\alpha \in \mathbb{F}_p$ and x^2+bx+c an irreducible monic quadratic polynomial in $\mathbb{F}_p[x]$. Now, there are $(p-1)$ choices for a, p choices for α. Next, we count the number of irreducible monic quadratic polynomials in $\mathbb{F}_p[x]$. The total number of monic quadratic polynomials is p^2. Any *reducible* quadratic polynomial is of the form $(x-a_1)(x-a_2)$ for $a_1, a_2 \in \mathbb{F}_p$. If a_1, a_2 are distinct, then there are $\binom{p}{2}$ such polynomials; if $a_1 = a_2$, then there are p such polynomials. So, the total number of irreducible monic quadratic polynomials are
$$p^2 - \binom{p}{2} - p = \binom{p}{2}$$
So, there are
$$(p-1)p\binom{p}{2} = \frac{p^2(p-1)^2}{2}$$
polynomials that belong to the first case.

(2) In the second case, the quadratic factor of $f(x)$ is *reducible*. So, in this case, $f(x)$ has three roots, i.e
$$f(x) = a(x-a_1)(x-a_2)(x-a_3)$$
for some $a \neq 0$, $a_1, a_2, a_3 \in \mathbb{F}_p$. Again, there are $(p-1)$ choices for a. If all of a_1, a_2, a_3 are distinct, then there are $\binom{p}{3}$ choices. If exactly two of a_1, a_2, a_3 are equal, then there are $2\binom{p}{2}$ choices. If $a_1 = a_2 = a_3$, then there are p choices. So, the total number of such polynomials are
$$(p-1)\left(p + 2\binom{p}{2} + \binom{p}{3}\right)$$

Because there are $(p-1)p^3$ total degree three polynomials over $\mathbb{F}_p[x]$, it follows that the total number of irreducible degree three polynomials in $\mathbb{F}_p[x]$ is
$$(p-1)p^3 - (p-1)p\binom{p}{2} - (p-1)\left(p + 2\binom{p}{2} + \binom{p}{3}\right)$$
Putting $p = 3$ in the above formula, we get that there are 16 irreducible degree three polynomials in $\mathbb{F}_3[x]$, and putting $p = 5$ we see that there are 160 irreducible degree three polynomials in $\mathbb{F}_5[x]$. ■