NEPAL ALGEBRA PROJECT 2018
MODULE 1 — HOMEWORK #1: SOLUTIONS
FRIDAY, 18^{th} MAY 2018

1. Obviously there are no real roots. The four complex roots are points z on the unit circle for which $x^4 = i = e^{\pi i}$. They are the points $e^{i\theta}$, with $\theta = \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}$, or in "Cartesian coordinates", the complex numbers $\alpha = \frac{\sqrt{2}}{2}(1+i), \beta = \frac{\sqrt{2}}{2}(-1+i), \overline{\beta} = \frac{\sqrt{2}}{2}(-1-i), \overline{\alpha} = \frac{\sqrt{2}}{2}(1-i)$. This gives the answer to (c):

$$X^4 + 1 = (X-\alpha)(X-\overline{\alpha})(X-\beta)(X-\overline{\beta})\,.$$

The factors are irreducible because they have degree one.

For (b), we pair each root with its complex conjugate, getting $(X-\alpha)(X-\overline{\alpha}) = X^2 - \sqrt{2}X + 1$ and $(X-\beta)(X-\overline{\beta}) = X^2 + \sqrt{2}X + 1$. This answers (b):

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1\,.$$

The factors are irreducible in $\mathbb{R}[X]$ because each has degree and has no real roots.

For (a), we guess that the polynomial is irreducible over $\mathbb{Q}$ and check it by substituting $X+1$ for X: $(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$, which is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion with $p = 2$, Therefore the original polynomial $X^4 + 1$ is irreducible over $\mathbb{Q}$.

Finally, (d). By Freshman's Dream, $(X+1)^2 = X^2+1$, and $(X^2+1)^2 = X^4+1$. This yields the factorization over $\mathbf{F}_2$:

$$X^4 + 1 = (X+1)^4\,.$$

The factors are irreducible because they are linear.

2. This problem was designed to give you a preview of Galois Theory, where you will learn systematic approaches to solving problems like this. At this point you really do not have these tools. There are two guiding principles here for an automorphism φ of a field F containing $\mathbb{Q}$:

GP1: $\varphi(c) = c$ for every $c \in \mathbb{Q}$. ("Elements of $\mathbb{Q}$ are fixed.")

GP2: If $\alpha \in F$ is a root of some polynomial $f(X) \in \mathbb{Q}[X]$, then $\varphi(\alpha)$ is also a root of $f(X)$. ("Roots map to roots.")

Proof of **GP1**: We know $\varphi(1) = 1$, so $\varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = 2$. In this boring fashion, we easily get $\varphi(n) = n$ for every positive integer n. Also, since φ is a homomorphism of additive groups, we have $\varphi(0) = 0$, and $\varphi(-n) = -\varphi(n) = -n$ for every positive integer n. Thus elements of $\mathbb{Z}$ are fixed. Finally, given a rational number q, write $q = \frac{a}{b}$, where a and b are integers, with $b \neq 0$. Then

$$b\varphi(q) = \varphi(b)\varphi(q) = \varphi(bq) = \varphi(a) = a\,,$$

so $\varphi(q) = \frac{a}{b} = q$.

Proof of **GP2**: Write $f(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$, with $a_i \in \mathbb{Q}$. Now $f(\alpha) = 0$, that is,

$$a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0\,.$$

Applying φ to both sides, we have (since φ preserves addition and multiplication)

$$\varphi(a_m)(\varphi(\alpha))^m + \varphi(a_{m-1})(\varphi(\alpha))^{m-1} + \cdots + \varphi(a_1)\varphi(\alpha) + \varphi(a_0) = \varphi(0)\,,$$

which, by **GP1**, simplifies to

$$a_m(\varphi(\alpha))^m + a_{m-1}(\varphi(\alpha))^{m-1} + \cdots + a_1\varphi(\alpha) + a_0 = 0\,.$$

This shows that $f(\varphi(\alpha)) = 0$, as desired.

(a) Since i is a root of X^2+1, whose other root is $-i$, any automorphism φ has to take $a+bi$ to either $a+bi$ or $a-bi$. The first case gives the identity map, and the second is complex conjugation. It is clear that the map $\varphi(a+bi) = a-bi$ preserves addition. Also, $\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i = (a-bi)(c-di) = \varphi(a+bi)\varphi(c+di)$. This shows that conjugation is a field homomorphism, and it's clearly injective and surjective. Summary: The two automorphisms are the identity and complex conjugation.

(b) Again, there are two automorphisms: The identity and the map taking $a+b\sqrt{2}$ to $a-b\sqrt{2}$. Any autormorphism has to take $\sqrt{2}$ to either $\sqrt{2}$ or $-\sqrt{2}$, the other root of X^2-2. The proof that the "conjugation" map taking $a+b\sqrt{2}$ to $a-b\sqrt{2}$ is an automorphism is pretty much the same as for part (a).

(c) The identity map is the only automorphism. To see this, let φ be any automorphism. Then $\varphi(\sqrt[3]{2})$ must be a root of X^3-2. But this polynomial has only one real root, and hence only one root in $\mathbb{Q}[\sqrt[3]{2}]$, namely $\sqrt[3]{2}$. So we have $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, and hence $\varphi(\sqrt[3]{4}) = \varphi((\sqrt[3]{2})^2) = (\varphi(\sqrt[3]{2}))^2 = (\sqrt[3]{2})^2 = \sqrt[3]{4}$. Therefore every element $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is fixed.

(d) As in (c), any automorphism φ is determined by the value $\varphi(\sqrt[4]{2})$, and this value must be another root of X^4-2. The four complex roots of X^4-2 are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$, and $\pm\sqrt[4]{2}$ are the only real roots, hence the only roots in the field $\mathbb{Q}[\sqrt[4]{2}]$. Therefore there are at mos two automorphisms. One can check directly (if one is a masochist) that the map

$$a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt{2}\sqrt[4]{2} \quad\mapsto\quad a - b\sqrt[4]{2} + c\sqrt{2} - d\sqrt{2}\sqrt[4]{2}$$

is an automorphism. Therefore there are exactly two automorphisms – the one just described and the identity map.

3. Well, the first two were too hard, but this one is too easy. Start the algorithm by dividing $f(X)$ by $g(X)$. The remainder is 0 (and the quotient is $X-1$). In other words, the GCD is $g(X)$ itself, and the desired linear combination is:

$$g(X) = 0\cdot f(X) + 1\cdot g(X)\,.$$

4. We have to show that $f^{-1}(J)$ and $f(I)$ are closed under (i) addition and (ii) negation, and that (ii) stable under multiplication by elements of R. First, we observe that $f(0) = 0$. To see this, we have

$$0 + f(0) = f(0) = f(0+0) = f(0) + f(0)\,,$$

so, adding, $-f(0)$ to both sides, we get $0 = f(0)$. Next, we observe that $f(-a) = -f(a)$ for every $a \in R$. To see this, we have

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a)\,,$$

so, adding $-f(a)$ to both sides, we get $-f(a) = f(-a)$. Now onward:

(a) Let $a, b \in f^{-1}(J)$, and let $r \in R$. Then $f(a) \in J$ and $f(b) \in J$.

(i) $f(a+b) = f(a) + f(b) \in J$. Therefore $a+b \in f^{-1}(J)$.

(ii) We have $f(-a) = -f(a) \in J$. Thus $-a \in f^{-1}(J)$.

(iii) $f(ra) = f(r)f(a) \in J$. Therefore $ra \in f^{-1}(J)$.

(b) Let $R = \mathbb{Z}$, $S = \mathbb{Q}$, and $F : \mathbb{Z} \to \mathbb{Q}$ the inclusion homomorphism taking $n \in \mathbb{Z}$ to $n \in \mathbb{Q}$. Then $I = \mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $f(I) = \mathbb{Z}$ is *not* an ideal of $\mathbb{Q}$. (Take $s = \frac{4}{23} \in S$ and $\alpha = 9 \in f(I)$. Then $s\alpha = \frac{36}{23} \notin \mathbb{Z} = f(I)$. Therefore $f(I)$ is not stable under multiplication by elements of S.)

5. For $0 < \ell < p$, let b denote the binomial coefficient $\binom{p}{\ell}$. We want to show that $p \mid b$. We have $b = \frac{p!}{\ell!(p-\ell)!}$, so $b \cdot \ell! = p(p-1)\dots(p-\ell+1)$. This shows that $p \mid b \cdot \ell!$. Now since $p \nmid i$ for $1 \leq i \leq \ell$, we must have $p \mid b$. (If a prime divides a product, it must divfide one of the factors.)

Let R be any commutative ring. Given a non-negative integer m, we also let m denote the element $m \cdot 1_R$ of R. For $0 \leq \ell \leq m$, the binomial coefficient $b = \binom{m}{\ell}$ therefore makes sense in R. (Just compute the integer b and then take the element $b \cdot 1_R$.) Moreover, the usual proof, by induction, of the Binomial Theorem, namely, $(a+b)^m = \sum_{\ell=0}^{m} \binom{m}{\ell} a^\ell b^{m-\ell}$, works in any commutative ring. In particular, in the ring $\mathbb{F}_p[X]$, we have $(f(X)+g(X))^p = \sum_{\ell=0}^{p} \binom{p}{\ell} f(X)^\ell g(X)^{p-\ell}$. By the first part of the problem, $\binom{p}{\ell} = 0$ for $0 < \ell < p$. Therefore only the 0th and pth terms survive, and we get the Freshman's Dream.