NAP 2018, ANNOUNCEMENTS, NOTES ON CLASS #2, AND HOMEWORK COMMENTARY

ANNOUNCEMENTS

- Preliminary Homework due today.
- Homework Assignment #1 due Tuesday, 10 pm, Nepal time.
- Tutors will be in this room tomorrow (Friday, 11 May), 4:30 – 6:30 pm. Come and ask them questions.

SUMMARY of CLASS #2, 09 May, 2018

- We asked students to read pages 6–13 in Milne (up through Remark 1.18) and learn the Euclidean Algorithm (1.8) for finding the GCD of two polynomials and expressing it as a linear combination of the two polynomials.
- Reminders concerning rings, fields, PIDs.
- Definition of ring homomorphism.
- $\mathbb{Z} \times \{0\}$ is an ideal of the ring $\mathbb{Z} \times \mathbb{Z}$. It's actually a ring with identity $(1, 0)$, but it's not a subring of $\mathbb{Z} \times \mathbb{Z}$, since its identity is not the same. (The identity element of $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$.)
- A field F has exactly two ideals, namely, $\{0\}$ and F. A commutative ring with exactly two ideals is a field.
- Field homomorphisms are always injective (one-to-one).
- Fields are integral domains.
- A finite integral domain is a field. (Proof: Let a be an arbitrary non-zero element of the finite integral domain R. We have to show a has an inverse in R. Look at the powers: $a, a^2, a^3, a^4, \ldots$. They can't all be distinct (since R is finite), so say $a^i = a^j$, with $i < j$. Then $a^i \cdot 1 = a^i = a^j = a^i \cdot a^{j-i}$. By cancellation (Milne's definition of "domain"), we have $a^{j-i} = 1$. Since $j - i - 1 \geq 0$ we can set $b = a^{j-i-1}$ and get $ab = 1$.)
- If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements, often denoted $\mathbf{F}_p$.
- The *prime subfield* of a field F is the smallest subfield of F. It's isomorphic either to some $\mathbb{F}_p$ (if the characteristic is p) or to $\mathbb{Q}$ (if the characteristic is 0).
- Defined "irreducible" element of a domain (not a unit, and every factorization involves a unit).
- For a field F, units of $F[X]$ are the polynomials of degree 0 (non-zero constant polynomials).
- For a field F a polynomial $f(X)$ is irreducible in $F[X]$ if and only if it cannot be written as a product of two polynomials of lower degree.
- Be careful: $2X^2 + 2$ is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$.
- A consequence of the Division Algorithm: Let F be a field, $f(X)$ a polynomial in $F[X]$, and c an element of F. Then $X - c \mid f(X) \iff f(c) = 0$. A further consequence: If $f(X)$ has degree 2 or 3, then $f(X)$ is irreducible if and only if $f(X)$ has no roots in F. But this fails for degrees bigger than 3. For example, $X^4 + 2X^2 + 1$ has no roots in $\mathbb{Q}$; but it's certainly not irreducible in $\mathbb{Q}[X]$, since $X^4 + 2X^2 + 1 = (X^2 + 1)^2$.

Date: 10 May, 2018.

HOMEWORK COMMENTARY

• Problem #1 is pretty reasonable and also quite instructive. Enjoy!

• Problem #2 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, and the problem is probably too hard. But see what you can do by applying the following two guiding principles, 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.")

GP3: If $F = \mathbb{Q}[\alpha]$, then φ is completely determined by what it does to α. That is, once you know $\varphi(\alpha)$, you know $\varphi(\beta)$ for every $\beta \in \mathbb{Q}[\alpha]$. (This really just amounts to the fact that φ is required to preserve the field operations.)

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 $f(X) = a_mX^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$, 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.

Armed with these three guiding principles, you can easily show that the only automorphisms of $\mathbb{Q}[i]$ are the identity and the complex conjugation map $a + bi \mapsto a - bi$. Of course you need to verify that complex conjugation is an automorphism. (Please don't bother to prove that the identity map is an automorphism. That's obvious!) The same sort of idea works will with (b). I won't spoil your fun with (c); you should find that one perfectly reasonable. For (d), you will get full credit if you simply say where your proposed automorphisms take a typical element displayed to the right of the equal sign. Don't bother to prove that it's an automorphism; that might be a bit grim, and soon you will learn a wonderful trick that does the work for you!

• Problem 3 is probably *too* easy. Just be sure you understand the definition of GCD, and you'll do fine.

• Problems 4 is just a matter of understanding the definitions. It proves itself.

• Problem 5, in particular, the Freshman's Dream, depends on the fact that the Binomial Theorem (suitably interpreted) works in any commurtative ring; just assume that.