HOMEWORK 9

Due date: Nov 27, Monday of Week 14

Exercise:1, (a), (d); 2 (2); 3; 4; 7; page 134;
Exercises: 1, 3, 8, page 139;

Comment: Let F be a field and $K \subset F$ be a subfield (some examples: $K = \mathbb{Q}, F = \mathbb{R}$; $K = \mathbb{R}, F = \mathbb{C}$; $K = \mathbb{Q}, F = \{a + b\alpha + c\alpha^2 : \alpha = \sqrt[3]{2}, a, b, c \in \mathbb{Q}\}$;). Let $f, g \in K[x]$ be two polynomials, and we can compute $\gcd_K(f, g)$ the greatest common divisor of f and g as elements in $K[x]$. On the other hand, $f, g \in F[x]$ since $K \subset F$. Thus we can also compute $\gcd_F(f, g)$, the greatest common divisor of f and g when they are viewed as elements in $F[x]$. Exercise 7, page 134 shows that

$$\gcd_K(f, g) = \gcd_F(f, g).$$

Please keep in mind this assertion. We will need this result later in this course.

Problem 1. *Try to find an irreducible polynomial of degree 2 and an irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$ and in $\mathbb{F}_3[x]$. How do you know they are irreducible? Justify your answer.*

Do this problem after Monday's class.

Problem 2. *Let F be a field and $K \subset F$ be a subfield. Then F can be viewed as a vector space over K. We have seen many examples like this in class and in previous HW. We assume that $\dim_K F = 2$ and F is algebraically closed. One such example is $K = \mathbb{R}$ and $F = \mathbb{C}$.*

1. *For any $\alpha \in F$, show that there exists a monic quadratic polynomial $f \in K[x]$ such that $f(\alpha) = 0$.*
2. *Show that any polynomial $g \in K[x]$ with $\deg(g) \geq 3$ is reducible. In particular, any $g \in \mathbb{R}[x]$ with $\deg(g) \geq 3$ is reducible.*

Comment: Given an algebraically closed field F (like $\mathbb{C}$), for any positive integer n, you might be wondering if there is a subfield K such that $\dim_K F = n$? In the example when $F = \mathbb{C}$ and $n = 2$, we know there is such a field K (which is $\mathbb{R}$) such that $\dim_K F = 2$. How about the general n? It seems that there is no familiar $K \subset \mathbb{C}$ such that $\dim_K \mathbb{C} = 3$ or 4 or any other positive integer. Actually, this is a general theorem. Namely, if K is a subfield of F with F algebraically closed and if $\dim_K F$ is finite, then $\dim_K F = 2$.

Comment: The fact "A polynomial $g \in \mathbb{R}[x]$ with $\deg(g) \geq 3$ must be reducible" is useful in the calculation of integrals of real rational functions (or fractions of real polynomials) in calculus class, where this fact is usually just assumed. Here you can give a proof on your own.

Problem 3. *Consider the polynomial $f = x^4 + 1 \in \mathbb{R}[x]$. We know that f is reducible by the above problem because it has degree 4. Factorize f into product of irreducible polynomials in $\mathbb{R}[x]$.*

Hint: There are many ways to do this. One way is to mimic the proof of the above problem. But to do so you need to know how to solve $x^4 + 1 = 0$ over $\mathbb{C}$.

You can do the above problems after Wednesday's class.

The following Theorem is a very useful criterion to show a polynomial in $\mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Theorem 0.1 (Eisenstein criterion)**.** *Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_i \in \mathbb{Z}$. Suppose that there is a prime number p such that all of the following 3 conditions are satisfied:*

1. *p divides a_i for each $0 \leq i < n$;*
2. *p does not divide a_n;*

(3) p^2 *does not divide* a_0.

Then $f(x)$ *is irreducible in* $\mathbb{Q}[x]$.

For example, $f(x) = 3x^4 + 15x + 10$ is indeed irreducible in $\mathbb{Q}[x]$ because Eisenstein criterion is applicable here with $p = 5$: 5 is prime; 5 divides $10, 15$ and 0 (0 is the coefficient of x^2 and also x^3); 5 does not divide 3 (coefficient of x^4); and 5^2 does not divide 10.

Another Example: We can use the above theorem to show

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

We cannot use Eisenstein criterion to $f(x)$ directly. Instead, we use Eisenstein criterion to $f(x+1)$. To simplify $f(x+1)$, note that $f(x) = \frac{x^5-1}{x-1}$. Thus $f(x+1) = \frac{(x+1)^5-1}{x}$, which can be easily simplified using binomial theorem. It is easy to see that 5 satisfies the condition given in the above theorem. Thus $f(x+1)$ is irreducible, which implies that $f(x)$ is irreducible. The following problem is a generalization of the above example. Using Eisenstein criterion, do the following problem

Problem 4. *Let* p *be a prime integer. Then the polynomial*

$$\Phi_p = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$$

is irreducible over $\mathbb{Q}$.

The polynomial Φ_p is called the p-th cyclotomic polynomial. It is an important object to study in number theory.

The proof of Eisenstein criterion will be given in a later course. You can use it in HW and even in exam if you think it is helpful. Its proof is not hard at all. Problem 2 can be done after Monday's class.

Problem 5. *Consider the polynomial* $p = x^3 - 2 \in \mathbb{Q}[x]$.

(1) *Show that* p *is irreducible. (You can use Eisenstein criterion).*

(2) *Let* $\alpha \in \mathbb{C}$ *be a root of* p. *Consider the set* $\mathbb{Q}[\alpha] := \left\{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\right\}$. *Show that the map* $\theta : \mathbb{Q}[x]/p\mathbb{Q}[x] \to \mathbb{Q}[\alpha]$ *defined by* $\theta(\overline{f}) = f(\alpha)$ *is well-defined, bijective, and satisfying*

$$\theta(c\overline{f} + \overline{g}) = c\theta(\overline{f}) + \theta(\overline{g}), \quad \theta(\overline{f}\,\overline{g}) = \theta(\overline{f})\theta(\overline{g}), \forall c \in \mathbb{Q}, \overline{f}, \overline{g} \in \mathbb{Q}[x]/p\mathbb{Q}[x].$$

(3) *Conclude that* $\mathbb{Q}[\alpha]$ *is indeed a field.*

(4) *Let* $\beta \in \mathbb{C}$ *and* $\beta \neq \alpha$ *be another root of* p. *Show that* $\mathbb{Q}[\beta] = \left\{a + b\beta + c\beta^2 : a, b, c \in \mathbb{Q}\right\}$ *is also a field and there is a bijective map* $\mathbb{Q}[\alpha] \to \mathbb{Q}[\beta]$ *which preserves addition and multiplication.*

You can do this Problem after Friday's class.