Homework
due on Wednesday, October 24

Problem 1. Find a greatest common divisor $d(x)$ of the polynomials $p(x) = x^3 + 4x^2 + x - 6$ and $q(x) = x^5 - 6x + 5$ in the ring $\mathbb{Q}[x]$ and find $a(x), b(x) \in \mathbb{Q}[x]$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

Solution: Dividing $x^5 - 6x + 5$ by $x^3 + 4x^2 + x - 6$ we get $x^2 - 4x + 15$ and remainder $-50x^2 - 45x + 95$. Thus

$$x^5 - 6x + 5 = (x^2 - 4x + 15)(x^3 + 4x^2 + x - 6) + (-50x^2 - 45x + 95)$$

Now divide $x^3 + 4x^2 + x - 6$ by $-50x^2 - 45x + 95$ to get

$$x^3 + 4x^2 + x - 6 = (\frac{-1}{50}x - \frac{31}{500})(-50x^2 - 45x + 95) + (\frac{11}{100}x - \frac{11}{100}).$$

Next divide $-50x^2 - 45x + 95$ by $\frac{11}{100}x - \frac{11}{100}$ to get

$$-50x^2 - 45x + 95 = (\frac{-5000}{11}x - \frac{9500}{11})(\frac{11}{100}x - \frac{11}{100}).$$

It follow that $d(x) = \frac{11}{100}x - \frac{11}{100}$. Working backwards, we have

$$d(x) = x^3 + 4x^2 + x - 6 - (\frac{-1}{50}x - \frac{31}{500})(-50x^2 - 45x + 95) =$$

$$x^3 + 4x^2 + x - 6 - (\frac{-1}{50}x - \frac{31}{500})(x^5 - 6x + 5 - (x^2 - 4x + 15)(x^3 + 4x^2 + x - 6)) =$$

$$(\frac{1}{50}x + \frac{31}{500})(x^5 - 6x + 5) + (\frac{-1}{50}x - \frac{31}{500})(x^2 - 4x + 15) + 1](x^3 + 4x^2 + x - 6) =$$

$$(\frac{1}{50}x + \frac{31}{500})(x^5 - 6x + 5) + (\frac{-1}{50}x^3 + \frac{9}{500}x^2 - \frac{26}{500}x + \frac{35}{500})(x^3 + 4x^2 + x - 6).$$

Problem 2. Let I be an ideal of the ring R. Define $I[x]$ as the subset of $R[x]$ which consists of all the polynomials in $R[x]$ whose all coefficients belong to I. Prove that $I[x]$ is an ideal of $R[x]$ and that $R[x]/I[x]$ is naturally isomorphic to the polynomial ring $(R/I)[x]$.

Solution: Let $f : R \longrightarrow R/I$ be the canonical homomorphism. Since R/I is a subring of $(R/I)[x]$ we can consider f as a homomorphism $f : R \longrightarrow (R/I)[x]$. By the universal property of polynomials rings, there exists unique homomorphism $f^* : R[x] \longrightarrow (R/I)[x]$ which agrees with f on the constants R and which sends x

to x. Explicitely, $f^*(p_0+p_1x+...+p_mx^m) = f(p_0)+f(p_1)x+...+f(p_m)x^m$. Since f is surjective, it is clear that f^* is surjective. A polynomial $p = p_0+p_1x+...+p_mx^m$ is in the kernel of f^* iff all coefficients of $f^*(p)$ are zero, i.e. iff $f(p_0) = f(p_1) = ... = f(p_m) = 0$. This means that all coefficients of p belong to $\ker f = I$, which by the definition of $I[x]$ means that $p \in I[x]$. We see that $\ker f^* = I[x]$. This proves in particular that $I[x]$ is an ideal (a direct verification of this fact is also quite simple). By the first isomorphism theorem, we get an isomorphism of $R[x]/I[x] = R[x]/\ker f^*$ and $(R/I)[x]$.

Problem 3. Let $R = \mathbb{Z}[\omega]$ be the ring of Eisenstein integers. Consider the homomorphism $f : \mathbb{Z}[x] \longrightarrow R$ such that $f(m) = m$ for $m \in \mathbb{Z}$ and $f(x) = \omega$ (there is unique such homomorphism by the result form class).

a) Prove that $\ker f = (x^2+x+1)\mathbb{Z}[x]$ and conclude that R is naturally isomorphic to the ring $\mathbb{Z}[x]/(x^2+x+1)\mathbb{Z}[x]$.

b) Prove that x^2+x+1 is a prime element in $\mathbb{Z}[x]$.

c) Prove that the ideal $M =< 2, x^2+x+1 >$ is not principal.

d) Prove that $\mathbb{Z}[x]/M$ and $R/2R$ are isomorphic. Conclude that M is maximal.

Solution: The homomorphism $f : \mathbb{Z}[x] \longrightarrow R$ is defined by $f(p_0+p_1x+...+p_mx^m) = p_0+p_1\omega+...+p_m\omega^m = p(\omega)$.

a) Clearly $f(1+x+x^2) = 1+\omega+\omega^2 = 0$ so $(x^2+x+1)\mathbb{Z}[x] \subseteq \ker f$. Suppose now that $p \in \mathbb{Z}[x]$ is an arbitrary polynomial. Since x^2+x+1 is monic, the division algorithm for polynomials implies that there are polynomials $h, r \in \mathbb{Z}[x]$ such that $p(x) = h(x)(x^2+x+1)+r(x)$ and the degree of r is smaller than 2. Thus $r(x) = ax+b$ for some integers a, b. It follows that

$$f(p) = p(\omega) = h(\omega)(\omega^2+\omega+1)+r(\omega) = a\omega+b.$$

Clearly, $f(p) = 0$ iff $a = b = 0$, i.e. iff $r = 0$. This proves that $p \in \ker f$ iff $x^2+x+1|p$, i.e. $\ker f = (x^2+x+1)\mathbb{Z}[x]$. Since $a+b\omega = f(a+bx)$ for any integers a, b, we see that f is surjective. By the first isomorphism theorem, R is isomorphic to the ring $\mathbb{Z}[x]/(x^2+x+1)\mathbb{Z}[x]$.

b) Since R is a domain, the ring $\mathbb{Z}[x]/(x^2+x+1)\mathbb{Z}[x]$ is a domain by a). Thus $(x^2+x+1)\mathbb{Z}[x]$ is a prime ideal which is non-zero, so x^2+x+1 is a prime element.

c) Since x^2+x+1 is a prime element, it is irreducible. Thus the ideal $(x^2+x+1)\mathbb{Z}[x]$ is maximal among proper principal ideals. Note that $2 \notin (x^2+x+1)\mathbb{Z}[x]$, so M is strictly bigger than $(x^2+x+1)\mathbb{Z}[x]$. If M were principal, it would not be a proper ideal, i.e. it would equal $\mathbb{Z}[x]$. But elements of M are of the form $2 \cdot p + (x^2+x+1)q$ for some polynomials $p, q \in \mathbb{Z}[x]$. It follows that the only constant polynomials in M are even numbers, so $M \neq \mathbb{Z}[x]$. This proves that M is not principal.

d) This is a starightforward consequence of the second isomorphism theorem. In fact, note that M contains the kernel of f. Furthermore, $f(M) = 2R$. In fact $2a + 2b\omega = f(2+2x)$ and $2+2x = 2(1+x) \in M$, so every elementt of $2R$ belongs to $f(M)$. Conversely, if $g \in M$ then $g = 2 \cdot p + (x^2+x+1)q$ for some polynomials $p, q \in \mathbb{Z}[x]$ so $f(g) = f(2 \cdot p + (x^2+x+1)q) = 2f(p) \in 2R$. Thus in the correspondence theorem, the ideal M of $\mathbb{Z}[x]$ corresponds to the ideal $2R$ of R. Therefore, by the second isomorphism theorem, the rings $\mathbb{Z}[x]/M$ and $R/2R$ are isomorphic. Recall now that 2 is irreducible in R and R is a PID, so $2R$ is maximal (by the result from last quiz). Thus $R/2R$ is a field and so is $\mathbb{Z}[x]/M$. Thus M is maximal. (Alternatively, recall that in the correrspondense theorem maximal ideals correspond to maximal ideals).