Winter 2018, Math 148: Week 3 Problem Set
Due: Friday, February 2nd, 2018
Factorization in Polynomial Rings

Discussion problems. The problems below should be completed in class.

(D1) *The polynomial ring* $\mathbb{Z}_n[x]$.

(a) Can you find a unit in $\mathbb{Z}_4[x]$ with positive degree?

(b) Which elements of $\mathbb{Z}_3[x]$ are units? For which n does this hold?

(c) For which n does $\mathbb{Z}_n[x]$ have zero-divisors?

(d) What is the highest degree a zero-divisor can have in $\mathbb{Z}_6[x]$? How about $\mathbb{Z}_n[x]$?

(e) Which elements of $\mathbb{Z}_4[x]$ are zero-divisors?

(f) Use the Euclidean algorithm to find the greatest common divisor of

$$f(x) = x^3 + 3x^2 + 2x - 1 \qquad \text{and} \qquad g(x) = x^3 - 2x + 1$$

in $\mathbb{Q}[x]$. Do the same in $\mathbb{Z}_5[x]$. How do you reconcile these differences?

(g) In view of part (f), what is the relationship in general between the greatest common divisor of two polynomials when computed over $\mathbb{Z}_p$ (for p prime) vs. over $\mathbb{Q}$?

(h) Find the common divisor of $2x$ and $4x$ over $\mathbb{Z}_6$ of highest degree.

(D2) *Factoring polynomials over* $\mathbb{Z}_n$.

(a) Find all roots of $3x + 3 = 0$ over $\mathbb{Z}_6$. Why is this surprising?

(b) Find a linear (i.e. degree 1) polynomial over $\mathbb{Z}_6$ with no solutions.

(c) Consider the polynomial $f(x) = x^2 - x = (x)(x - 1)$ over $\mathbb{Z}_6$. Find all roots of $f(x)$ and the roots of its factors x and $x - 1$. What do you notice?

(d) Find all factorizations of $f(x) = x^2 - x$ over $\mathbb{Z}_6$.

(e) Factor $x^3 + 3x + 1$ and $x^3 + 3x^2 + 2x + 4$ over $\mathbb{Z}_5$ as a product of irreducibles.

(f) Factor $x^4 + 5$ over $\mathbb{Z}_3$. Does it factor over $\mathbb{Q}$?

(g) Factor $x^4 + 4$ over $\mathbb{Z}_5$. Does it factor over $\mathbb{Q}$? (The answer may surprise you!)

(h) Factor $x^5 + 1$ over $\mathbb{Z}_3$. Do the same over $\mathbb{Z}_5$. Where have you seen this before?

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Consider the polynomials $f(x) = x^5 + 3x^4 - 7x^3 + 5x + 4$ and $g(x) = 2x^2 + x + 5$. Divide $f(x)$ by $g(x)$ over $\mathbb{Z}_3$. Do the same over $\mathbb{Z}_{11}$. Without performing long division, decide whether $g(x)$ divides $f(x)$ over $\mathbb{Q}$.

(R2) Find the greatest common divisor of $f(x) = x^6 + x^4 + x^2$ and $g(x) = x^4 + x^3 + x$ over $\mathbb{Z}_3$. Would your answer be different over $\mathbb{Q}$?

(R3) Factor $f(x) = x^3 + 6x^2 + 1$ over $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_7$. Does it factor over $\mathbb{Q}$?

(R4) Factor $f(x) = x^5 + 4x^4 + 8x^3 + 11x$ over $\mathbb{Q}$. Hint: first try to factor $f(x)$ over some small finite fields, like $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) Consider the set $R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] : a_0 \in \mathbb{Z}\}$ of polynomials over $\mathbb{Q}$ with integer constant term.

  (a) Show that R is a ring under the usual addition and multiplication of polynomials.

  (b) Show that some elements of R cannot be factored into a finite product of irreducibles. Hint: consider the element $f(x) = x$.

(S2) Consider the set $R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] : a_1 = 0\}$ of polynomials over $\mathbb{Q}$ with no linear term.

  (a) Show that R is a ring under the usual addition and multiplication of polynomials.

  (b) Show that there are elements of R that can be factored in more than one distinct way. Hint: consider the element $f(x) = x^6$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Prove that any finite ring with no zero-divisors is a field.