MATH 371 – Homework 6– October 16, 2013

1. (a) Let $\varphi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Prove that $\ker(\varphi) \subset R$ is a prime ideal.

(b) Let I and J be ideals of R and P be a prime ideal of R. Prove that if $IJ \subset P$ then either $I \subset P$ or $J \subset P$.

(c) Suppose R is a principal ideal domain. Prove that every ideal in the quotient ring R/I is principal.

---

2. Is the ring $\mathbb{Z}[\sqrt{-2}]$ a Euclidean domain? How about $\mathbb{Z}[\sqrt{-3}]$? How about $\mathbb{Z}[\sqrt{-5}]$?

---

3. Prove there are infinitely many prime numbers congruent to 3 mod 4 (see the end of the notes on rings for primes congruent to 1 mod 4).

---

4. Let p be a prime integer. Define

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{s} \in \mathbb{Q} \mid p \nmid s \right\} \subset \mathbb{Q}.$$

(a) Prove that $\mathbb{Z}$ is a subring of $\mathbb{Z}_{(p)}$ and that $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$. What is the field of fractions of $\mathbb{Z}_{(p)}$?

(b) What are the units in $\mathbb{Z}_{(p)}$?

(c) Show that every non-zero element $\alpha \in \mathbb{Z}_{(p)}$ can be written uniquely as up^n where u is a unit and $n \geqslant 0$.

(d) Let I be a non-zero ideal of $\mathbb{Z}_{(p)}$. Show that $I = \langle p^n \rangle$ for some $n \geqslant 0$.

(e) Show that $\mathbb{Z}_{(p)}$ contains only one maximal ideal.

---

5. Show that $R[x]$ is an integral domain if R is an integral domain.

---

6. (a) Suppose the rational number $\alpha = a/s$, where a and s where $\gcd(a, s) = 1$. Show that if α is a root of the polynomial

$$a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

then $a \mid a_0$ and $s \mid a_n$.

(b) Prove that if a rational number α is a root of a *monic* polynomial in $\mathbb{Z}[x]$, then $\alpha \in \mathbb{Z}$.

(c) Generalize this to the case where R is a unique factorization domain and F is its field of fractions (so the conclusion is that if $\alpha \in F$ is a root of a monic polynomial in $R[x]$ then in fact $\alpha \in R$).

7. (a) Show that if p is prime then $\Phi_p(x) = x^{p-1} + \cdots + x + 1$.

(b) Show that if p is prime then $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.

(c) Show that if $n \geqslant 3$ is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.

---

8. Let $\varphi\colon R \to S$ be a ring homomorphism. Prove that $\overline{\varphi}\colon R[x] \to S[x]$ given by

$$\overline{\varphi}(a_n x^n + \cdots + a_1 x + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$$

is a ring homomorphism.

---

9. (a) Calculate $\Phi_8(x)$.

(b) Show that Φ_8 is reducible in $\mathbb{F}_p[x]$ for $p \equiv 1 \pmod 4$.

(c) Suppose that $p \equiv 3 \pmod 8$. Show that there is an element $a \in \mathbb{F}_p$ such that $a^2 = -2$ (maybe you don't have to find a to do this!). Prove for such a value of a that $\Phi_8 = (x^2 + ax - 1)(x^2 - ax - 1)$ in $\mathbb{F}_p[x]$.

(d) Now suppose $p \equiv 7 \pmod 8$. Show that there is an $a \in \mathbb{F}_p$ such that $a^2 = 2$. Prove for such a value of a that $\Phi_8 = (x^2 + ax - 1)(x^2 - ax - 1)$ in $\mathbb{F}_p[x]$.

(e) Conclude that Φ_8 is reducible in $\mathbb{F}_p[x]$ for all prime numbers p.

---

10 (from class, 10/17): We know that there is, up to isomorphism, one field with $8 = 2^3$ elements. There are two irreducible cubic polynomials in $\mathbb{F}_2[x]$, namely $p = x^3 + x^2 + 1$ and $q = x^3 + x + 1$. Therefore $E = \mathbb{F}_2[x]/\langle p\rangle$ and $E' = \mathbb{F}_2[x]/\langle q\rangle$ are both fields of order 8. Describe these fields explicitly and then find the isomorphism $\varphi\colon E \to E'$.