Mathematics GU4042
Introduction to Modern Algebra II

Assignment #4

Due February 17, 2017

1. How many roots does $x^3 - x$ have in $\mathbf{Z}_6$? Why does this not contradict any theorems from class?

2. Prove that any root in $\mathbf{Q}$ of a monic $f(x) \in \mathbf{Z}[x]$ is actually in $\mathbf{Z}$.

3. (a) Does an irreducible $n \in \mathbf{Z}$ have to remain irreducible in the Gaussian integers $\mathbf{Z}[i]$? Give a proof or counterexample.

(b) In $\mathbf{Z}[i]$, show that if $(a + bi) \mid n \in \mathbf{Z}$, then $(a - bi) \mid n$ too.

(c) For $m, n \in \mathbf{Z}$, show that $d \in \mathbf{Z}$ is their greatest common divisor in $\mathbf{Z}$ if and only if it is their greatest common divisor in $\mathbf{Z}[i]$.

4. In the ring $\mathbf{Q}[x, y]$, prove that $xy + 1$ is irreducible. Hint: regard $\mathbf{Q}[x, y]$ as polynomials in one variable with coefficients in the other, and consider degrees in any possible reduction.

5. (a) Euclid proved that there are infinitely many prime numbers in $\mathbf{N}$ as follows: if only finitely many primes $p_1, \ldots, p_k$ exist, then any prime factor of $p_1 p_2 \cdots p_k + 1$ cannot divide $p_1 p_2 \cdots p_k$, hence is a new prime not on the list, contradiction. Adapt this proof to show that, for any field F, there are infinitely many monic irreducible polynomials in $F[x]$.

(b) For any prime number p and any $k > 0$, show that there exists a finite field F satisfying $p^k \mid \#F$.

6. In a Euclidean domain, say that two elements are *coprime* if 1 is a gcd.

(a) In a Euclidean domain, prove that x, y are coprime if and only if there exist a, b such that $ax + by = 1$.

(b) Prove that $f(x), g(x) \in \mathbf{Z}[x]$ are coprime in $\mathbf{Q}[x]$ if and only if the ideal $(f, g) \subset \mathbf{Z}[x]$ contains a nonzero integer.

7. Let $\alpha \in \mathbf{C}$. For $\phi : \mathbf{Z}[x] \to \mathbf{C}$ given by $\phi(f) = f(\alpha)$, prove that $\ker \phi$ is a principal ideal.