ALGEBRA 611, FALL 2009. HOMEWORK 5 [1]

In this worksheet p denotes a prime number, k denotes an arbitrary field, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denotes a finite field with p elements, R denotes a ring, and R^* denotes the multiplicative group of units of R.

1. Let $R = \mathbb{Z}[i] \subset \mathbb{C}$. (a) Draw the principal ideal $(1+3i)$ (as a subset of the complex plane). (b) Let $a, b \in R$. Prove that in R one can write $a = bq + r$, where $0 \le |r| < |b|$. (c) Prove that R is a PID (and hence a UFD). (d) Find the factorization of 15 into irreducible elements of R.

2. Let $R = \mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$. (a) Draw the principal ideal generated by $2+\sqrt{-2}$. (b) Prove that R is a UFD. (c) Prove that if $x, y \in \mathbb{Z}$ such that $y^2 + 2 = x^3$, then $y + \sqrt{-2}$ is a cube in R. (d) Determine all integer solutions of the diophantine equation $y^2 + 2 = x^3$.

3. Prove that a finite domain is a field.

4. Prove that if R is a PID and $d \in R$ is irreducible then $R/(d)$ is a field.

5. Prove that $k[x]$ contains infinitely many irreducible polynomials.

6. Suppose R contains $\mathbb{F}_p$. Prove that the map

$$F : R \to R, \quad F(x) = x^p$$

is a ring homomorphism (called the Frobenius endomorphism).

7. Fix an integer $m > 0$. (a) Prove that $\mathbb{F}_p[x]$ contains an irreducible polynomial f of degree $n > m$. (b) Show that $\mathbb{F}_{p^n} := \mathbb{F}_p[x]/(f)$ is a field with p^n elements. (c) Suppose that m divides n. Show that

$$\mathbb{F}_{p^m} := \{x \in \mathbb{F}_{p^n} \mid x^{p^m} = x\}$$

is a subfield with p^m elements (Hint: use that $\mathbb{F}^*_{p^n}$ is a cyclic group).

9. Find all Sylow subgroups of $R = \mathbb{Z}/72\mathbb{Z}$ (as an additive group) and R^*.

10. Let R be the ring of p-adic integers (the inverse limit of rings $\mathbb{Z}/p^n\mathbb{Z}$). (a) Prove that R is a domain. (b) Prove that $a \in R^*$ iff $a \not\equiv 0 \mod p$ (Hint: this is analogous to $k[[x]]$). (c) Describe all ideals in R.

11. Consider $\mathbb{Q}$ (rational numbers) as an Abelian group. (a) Prove that $\mathbb{Q}$ is not a direct sum of cyclic groups. Does this contradict the fundamental theorem on Abelian groups? (b) Suppose $\mathbb{Q}$ is contained in an Abelian group G. Prove that G contains a nontrivial subgroup H such that $\mathbb{Q} \cap H \neq \{0\}$. Then use Zorn's lemma to prove that G contains a nontrivial subgroup H such that $\mathbb{Q} \oplus H = G$.

---

[1] This homework is due before class on Monday Nov 2. These problems will be discussed during the review section on Monday at 4pm. The grader will grade 5 random problems from this assignment. A problem with multiple parts (a), (b), etc. counts as one problem. Please make sure that all solutions are complete and accurately written. There is a "bail-out" provision: you can ask the grader not to grade *two* of the problems. Please indicate clearly in the beginning of your homework which problems you don't wish to be graded.