FIELD THEORY HOMEWORK SET I

JAMES CUMMINGS

You may collaborate on this homework set, but must write up your solutions by yourself. Please contact me by email if you are puzzled by something, would like a hint or believe that you have found a typo.

(1) Let R be an ID and let P be a prime ideal of R. Let F be the field of fractions of R, and let S be the subset of F consisting of elements that can be written in the form a/b where $a \in R$, $b \in R \setminus P$.
  (a) Prove that S is a subring of F, and that R is contained in S (as usual, each $r \in R$ is identified with the fraction $r/1$ in F).
  (b) Prove that the units of S are precisely the elements of form a/b where $a, b \in R \setminus P$.
  (c) Prove that the set of nonunits in S forms an ideal.
  (d) Prove that the set of nonunits is the only maximal ideal in S.
  (e) Suppose now that $R = \mathbb{Z}$, $F = \mathbb{Q}$ and $P = (p)$ for some prime number p.
  Prove that
    (i) p and its associates are the only irreducibles in S.
    (ii) The only ideals in S are those of form (p^n) for $n \geq 0$.

(2) Let $R = \mathbb{Z}[i]$, the least subring of the complex numbers containg $\mathbb{Z}$ and i.
  (a) Show that R consists of all complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$.
  (b) Show that if $a+bi \neq 0$ then the principal ideal $(a+bi)$, when considered as a subset of the complex plane, forms a square lattice. Deduce that R is a Euclidean domain (hint: use the absolute value as your Euclidean function).
  (c) Let $N(a+bi) = a^2+b^2$. Show that $N(rs) = N(r)N(s)$ for all $r, s \in R$. Show that the units of R are precisely those $r \in R$ with $N(r) = 1$, and identify them.
  (d) Show that $N(r)$ is never congruent to 3 modulo 4. use this to show that if the prime number p is congruent to 3 modulo 4, then p is prime in R.
  (e) Show that 5 is not prime in R, and find its prime factorisation.

(3) Let $\alpha = i\sqrt{5}$, and let $R = \mathbb{Z}[\alpha]$, the least subring of the complex numbers containg $\mathbb{Z}$ and α.
  (a) Show that R consists of all complex numbers of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$.
  (b) Let $N(a + b\alpha) = a^2 + 5b^2$. Show that $N(rs) = N(r)N(s)$. Show that the units of R are precisely those $r \in R$ with $N(r) = 1$, and identify them.
  (c) Show that $2, 3, 1 + \alpha, 1 - \alpha$ are all irreducible in R.
  (d) Show that R is not a UFD. Hint: what is $(1 + \alpha)(1 - \alpha)$?

   (e) Show that $2, 3, 1+\alpha, 1-\alpha$ are not prime in R.
(4) Prove that the identity map is the only automorphism of the field $\mathbb{R}$.
(5) Let $\mathbb{Q}(i)$ be the least subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and i, and $\mathbb{Q}[i]$ be the least subring of $\mathbb{C}$ containing $\mathbb{Q}$ and i. Prove that $\mathbb{Q}(i) = \mathbb{Q}[i]$.
(6) Recall that S_4 is the group of all permutations of the set $\{1, \ldots 4\}$. Find all the subgroups of S_4, and indicate which ones are normal.