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).

This is tedious, the main point is that the set of denominators is closed under multiplication (as P is a prime ideal).

(b) Prove that the units of S are precisely the elements of form a/b where $a, b \in R \setminus P$.

If a/b is of this form then $b/a \in S$, and is the inverse. Conversely suppose that a/b is a unit in S, where $b \notin P$. Then $b/a \in S$, so $b/a = b'/a'$ where $a' \notin P$. We have the equation $b'a = ba' \notin P$ since P is prime, so $b' \notin P$ and we are done.
Note: I had to be a bit careful because an element of the FOF can have many representations as a fraction. In particular an element of S can have representations where the denominator is in P.
Note: If R is not a PID there is in general no reasonable way to choose a “canonical” way of representing a member of the FOF.

(c) Prove that the set of nonunits in S forms an ideal.

The nonunits are elements of the form a/b for $a \in P, b \notin P$. These easily are seen to form an ideal.

(d) Prove that the set of nonunits is the only maximal ideal in S.

Any ideal which contains a unit is the whole ring, so any ideal $I \neq S$ is contained in the set of nonunits. Hence the set of nonunits is maximal, and is the only maximal ideal.

(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 $n \geq 0$.

By prime factorisation every element is an associate of p^n for some $n \geq 0$. So it is enough to work out which of these elements are irreducible. Again by prime factorisation we see that p is the only irreducible.

Now let I be an ideal and let n be least such that $p^n \in I$. Then I contains all multiples of p^n but no associates of p^m for $m < n$, so that easily $I = (p^n)$.

Cultural comment: This is a foretaste of the theory of local rings and DVR's, which are important in more advanced work in algebra.

(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 $a, b \in \mathbb{Z}$.

Routine once we note that $i^2 = -1 \in \mathbb{Z}$.

(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).

Recall that in the complex plane the number $a + bi$ is identified with the point (a, b). Also $i(a + bi) = -b + ai$, which is identified with the point $(-b, a)$ obtained by rotating (a, b) through a right angle about 0. Now it is easy to see that (a, b) and $(-b, a)$ generate a square lattice. To finish let $a + bi$ be nonzero and let $c + di$ be arbitrary. Then in the complex plane the point $c + di$ must be within $\sqrt{2}/2|a + bi|$ of some point of the square lattice of points $(a + bi)$; so we can find $q \in R$ such that $|(c + di) - q(a + bi)| < |a + bi|$.

(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.

The multiplicative property of N is routine. Note that $N(z) = z\bar{z}$ where $\bar{z}$ is the complex conjugate of z.
If r is a unit then $rs = 1$ so $N(r)N(s) = 1$ and so $N(r)$ is a unit in $\mathbb{Z}$. But N is a positive function so $N(r) = 1$. Conversely if $N(r) = r\bar{r} = 1$ then $\bar{r} \in R$, so $\bar{r}$ is an inverse and r is a unit.
The units are $1, -1, i, -i$.

(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.

For any integer a, a^2 is congruent to zero or one mod four. Now let $p \equiv 1 \mod 4$, and suppose that p is not prime in R. Since R is Euclidean it's a PID, so primeness is irreducibility. Let $p = ab$ where a, b are not units in R, then $p^2 = N(p) = N(a)N(b)$ so $N(a) = N(b) = p$. But this is impossible,

(e) Show that 5 is not prime in R, and find its prime factorisation.

$5 = (2 + i)(2 - i)$. $N(2 + i) = 5$ which is prime, so arguing as in the also question $2 + i$ is prime. Similarly $2 - i$ is prime.

(3) Let $\alpha = i\sqrt{5}$, and let $R = \mathbb{Z}[\alpha]$, the least subring of the complex numbers containingg $\mathbb{Z}$ and α.

(a) Show that R consists of all complex numbers of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$.

Follows easily from $\alpha^2 = -5 \in \mathbb{Z}$.

(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.

Again $N(z) = z\bar{z}$. Much as in the last question we get that the units are $1, -1$.

(c) Show that $2, 3, 1 + \alpha, 1 - \alpha$ are all irreducible in R.

Consider the function N mod 5 and observe that $N(a + b\alpha) \equiv a^2 \equiv 0, 1, 4 \mod 5$. Now $N(2) = 4 = 2 \times 2,$, $N(3) = 9 = 3 \times 3$, $N(1 \pm \alpha) = 2 \times 3$, so argue as in the last question that they are all irreducible.

(d) Show that R is not a UFD. Hint: what is $(1 + \alpha)(1 - \alpha)$?

$(1 + \alpha)(1 - \alpha) = 2 \times 3$ so that 6 has distinct factorisations into irreducibles.

(e) Show that $2, 3, 1 + \alpha, 1 - \alpha$ are not prime in R.

2 divides 6 but it divides neither of $1 \pm \alpha$. Similarly for the others.

(4) Prove that the identity map is the only automorphism of the field $\mathbb{R}$.

Let π be an AM. π fixes 1, so by an easy induction it fixes all elements of $\mathbb{N}$. It preserves inverses so it fixes all elements of $\mathbb{Z}$. It preserves quotients so it fixes all elements of $\mathbb{Q}$.

Now let $r > 0$, then $r = s^2$ so $\pi(r) = \pi(s^2) = \pi(s)^2 > 0$. So π preserves positivity. Then if $a < b$ we have $b - a > 0$, $\pi(b - a) = \pi(b) - \pi(a) > 0$, so π preserves the ordering.

Now let $r \in \mathbb{R}$. For every rational q, if $q < r$ then $q = \pi(q) < \pi(r)$, similarly if $r < q$ then $\pi(r) < q$. So $\pi(r) = r$.

(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 $\mathbb{Q}(i) = \mathbb{Q}[i]$.

As usual $\mathbb{Q}[i]$ is the set of $a + bi$ with $a, b \in \mathbb{Q}$. We need to see this is a field. So let $a + bi$ be a nonzero element and note that

$$\frac{1}{a + bi} = \frac{a - bi}{(a - bi)(a + bi)} = \frac{a - bi}{a^2 + b^2} \in \mathbb{Q}[i].$$

(6) Recall that S_4 is the group of all permutations of the set $\{1, \dots 4\}$. Find all the subgroups of S_4, and indicate which ones are normal.

By Lagrange the possible order for subgroups are $1, 2, 3, 4, 6, 8, 12, 24$.

Order 1: $\{e\}$.

Order 2: such subgroups are generated by elements of order 2. There are several of these, namely the 6 transpositions and the 3 elements $(12)(34)$, $(13)(24)$, $(14)(23)$.

Order 3: such subgroups are generated by elements of order 3. These are the 3-cycles, of which there are 8, giving 4 subgroups.

Order 4: such subgroups are either cyclic of order 4 or are Klein 4-groups (that is of form C_2^2).

The elements of order 4 are the 4-cycles, of which there are 6. This gives 3 cyclic groups of order 4.

The 4-groups consist of elements of order 2. These come in two kinds: there is $\{e, (12), (34), (12)(34)\}$ and two similar groups, but also the group $\{e, (12)(34), (13)(24), (14)(23)\}$.

Order 6: There are four copies of S_3, given by the permutation groups on the three-element subsets of $\{1, 2, 3, 4\}$. One can check that this is all.

Order 8: recall that the dihedral group of order 8 is the group od symmetries of the square. There are 3 subgroups of order 8, all of this kind. A typical one is generated by (1234) and (12)(34).

Order 12: there is the single subgroup A_4.

Of these the only non-trivial normal ones are A_4 and the subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$.