HOMEWORK 10, DUE THU APR 15TH

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let A be a PID. A module D is called *divisible* if for any non-zero $a \in A$, the multiplication map $D \xrightarrow{a} D$ is onto.

(a) Show that K, the fraction field of A (which is naturally an A-module) is divisible. Also, if D is divisible, any quotient module of D is divisible.

Solution. Given any $x \in D$, we can take $y = x/a \in K$, since $a \neq 0$. Then $ay = x$, which says the multiplication map is onto. Let $\pi : D \to E$ be any quotient module, so π is onto. Given $x \in E$, lift it to $x' \in D$, so that $\pi(x') = x$. Then, we have $y' \in D$ with $ay' = x'$ and then $a\pi(y') = x$. □

(b) Let $N \subset M$ are modules and let $f : N \to D$ is a homomorphism, where D is divisible. Show that there is a homomorphism $g : M \to D$ such that $g(n) = f(n)$ for all $n \in N$. (Hint: You will need Zorn's lemma).

Solution. Consider the collection consisting of (K, g_K) where $N \subset K \subset M$, K a submodule of M and $g_K : K \to D$ is an A-module homomorphism such that $g_K(n) = f(n)$ for all $n \in N$.This set is non-empty, since it contains (N, f). We introduce a partial order on this collection by saying $(K, g_K) \leq (L, g_L)$ if $K \subset L$ and $g_L(k) = g_K(k)$ for all $k \in K$. Easy to see that this is a partial order.
Now, let (K_i, g_{K_i}) be a totally ordered subset (and I will take $i \in \mathbb{N}$ for convenience of writing, but any totally ordered indexing set will do.) so that $K_i \subset K_{i+1}$ and $g_{K_{i+1}}(x) = g_{K_i}(x)$ for all $x \in K_i$.Then, let $L = \cup K_i$ and define $g : L \to D$ by $g(x) = g_{K_i}(x)$ if $x \in K_i$. You can see that the map does not depend on which K_i we pick containing x. Then (L, g) is in our set and is maximal for the K_is since it contains all of them.

So, Zorn's lemma applies and thus we have a maximal element (P, g) in our set. If $P = M$, we are done. So, assume not. Pick an $m \in M$, not in P. Let $Q = P + Am$, the submodule generated by P and m. We will extend g to Q, contradicting maximality of (P, g). There are two cases. Either the ideal $I = \{a \in A | am \in P\}$ is zero or non-zero.

If $I = 0$, we see that any element in Q can be *uniquely* written as $p + qm$ for some $p \in P, q \in A$. Then define $g' : Q \to D$ by $g'(p + qm) = g(p)$. I will leave you to verify that this does give an extension.

Next, assume that $I \neq 0$ and then $I = qA$ for some $0 \neq q \in A$, since A is a PID. Let $qm = p \in P$. Let $x = g(p)$ and let $y \in D$ be such that $qy = x$. Define $g' : Q \to D$ by $g'(p + am) = g(p) + ay$. I will leave you to check that this is well defined and thus gives an extension. □

(c) If D is a divisible module and is a submodule of a module M, show that there is a submodule $N \subset M$ such that $N \oplus D \cong M$. (This means, $N + D = M, N \cap D = 0$).

Solution. Consider the map $D \to D$, identity. By the previous problem, we get a homomorphism $g : M \to D$ such that $g(x) = x$ for all $x \in D$. Let $N = \operatorname{Ker} g$. Easy to check that $N + D = M$ and $N \cap D = 0$. □

(d) Let $M = A/pA$ where $p \in A$ is a prime. Show that M is the submodule of some divisible module.

Solution. Let K be the fraction field of A, which we know is divisible. So, $D = K/A$ is also divisible. Consider the element $x \in K/A$ which is the image of $\frac{1}{p} \in K$. We have a module homomorphism $A \to D$, by sending $1 \mapsto x$. Since $px = 0$, we see that the kernel of this map is precisely pA and thus we have an inclusion $A/pA \subset D$. □

(2) We consider the filed extension, $\mathbb{Q} \subset \mathbb{R}$.

(a) Show that $\sqrt{2}, \sqrt{3} \in \mathbb{R}$ are algebraic over $\mathbb{Q}$. Find a polynomial $P(X) \in \mathbb{Q}[X]$ of degree 4 such that $P(\sqrt{2} + \sqrt{3}) = 0$. Decide whether this polynomial is irreducible over $\mathbb{Q}$.

Solution. Since $\sqrt{2}$ is a root of $X^2 - 2 \in \mathbb{Q}[X]$, we see that it is algebraic and similarly for $\sqrt{3}$. Let $u = \sqrt{2} + \sqrt{3}$. We have, $u^2 = 5 + 2\sqrt{6}$. So, $(u^2 - 5)^2 = 24$, or $u^4 - 10u^2 + 1 = 0$. So, we get $Q(u) = 0$ where $Q(X) = X^4 - 10X^2 + 1$.

There are many ways of proving Q is irreducible. Let me do it the naive way. If it is not irreducible, either it has a linear factor or all factors of degree greater than one. In the former case, Q has a root $t \in \mathbb{Q}$. Then, $t^2 \in \mathbb{Q}$ and t^2 is a root of the quadratic polynomial $Y^2 - 10Y + 1$. But, quadratic formula tells us that the roots of this polynomial are $\frac{10 \pm \sqrt{100-1}}{2}$ and then $\sqrt{99} = 3\sqrt{11} \in \mathbb{Q}$, which is not true. So, Q must factor as product of two quadratic polynomials, say $X^2 + aX + b, X^2 + cX + d$. Multiplying, we get $X^4 + (a+c)X^3 + (ac + b + d)X^2 + (ad + bc)X + bd$. Thus, $c = -a, a(d-b) = 0, bd = 1$. If $a = 0$, we have $c = 0$ and $b + d = -10$ and $bd = 1$, which is impossible (again by quadratic formula, since this gives $b^2 + 10b + 1 = 0$). So, $a \neq 0$ and then $b = d$. So, $b = d = 1$ or $b = d = -1$. Then, we get, since $ac + bd = -10$, $-a^2 + 2 = -10$ or $-a^2 - 2 = -10$ and these give $a^2 = 12$ or $a^2 = 8$, neither is possible with $a \in \mathbb{Q}$.

□

(b) Show that $\sqrt{2} + \sqrt[3]{5}$ is algebraic over $\mathbb{Q}$ of degree 6.

Solution. The idea is the same. Let $u = \sqrt{2} + 5^{1/3}$. Then, $(u - \sqrt{2})^3 = 5$, which gives, $u^3 - 3\sqrt{2}u^2 + 6u - 2\sqrt{2} = 5$. Thus, $u^3 + 6u - 5 = \sqrt{2}(3u^2 + 2)$. Squaring, we get, $(u^3 + 6u - 5)^2 = 2(3u^2 + 2)^2$. Elementary algebra gives us a polynomial of degree 6 satisfied by u.

□

(3) We say an element in $a \in \mathbb{C}$ is an algebraic *integer*, if it satisfies an equation $a^n + a_1 a^{n-1} + \cdots + a_n = 0$ where $a_i \in \mathbb{Z}$. For example, $\sqrt{-1}, 2^{\frac{1}{5}}$ are algebraic integers.

(a) Show that if $a \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, there is some positive integer N such that Na is an algebraic integer.

Solution. If a is algebraic, we have an equation $a^n + a_1 a^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathbb{Q}$. Choose a positive integer

N such that Na_is are integers for all i. Multiplying the above equation by N^n, we get,

$$(Na)^n + Na_1(Na)^{n-1} + N^2a_2(Na)^{n-2} + \cdots + N^n a_n = 0.$$

Since Na_is are integers, we see that Na is an algebraic integer. □

(b) If $a \in \mathbb{Q}$ is an algebraic integer, show that $a \in \mathbb{Z}$.

Solution. If $r \in \mathbb{Q}$ an algebraic integer with an equation $r^n + a_1 r^{n-1} + \cdots + a_n = 0$ where $a_i \in \mathbb{Z}$, write $r = a/b$ with a, b integers as usual and $\gcd(a, b) = 1$. Then, multiply the above by b^n to get, $a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0$. Notice all the terms are integers now and all the terms after the first is divisible by b and so $b|a^n$. Since $\gcd(a, b) = 1$, this says $b = 1$ and thus r is an integer. □

(c) If a is an algebraic integer, show that the ring $\mathbb{Z}[a]$ is a finitely generated module over $\mathbb{Z}$.

Solution. If a satisfies an equation $a^n + a_1 a^{n-1} + \cdots + a_n$, one checks that $1, a, a^2, \ldots, a^{n-1}$ generate $\mathbb{Z}[a]$ as a $\mathbb{Z}$- module. □

(d) Show that if a, b are algebraic integers, so are $a + b, ab$. (Do not attempt to find the polynomials satisfied by these.)

Solution. Very much like what we did for fields, if $\mathbb{Z}[a]$ is generated by $e_1, \ldots, e_m$ as a $\mathbb{Z}$- module and similarly $v_1, \ldots, v_m$ generates $\mathbb{Z}[b]$, one easily checks that $\{e_i v_j\}$ generate $\mathbb{Z}[a, b]$ and since $\mathbb{Z}[a + b] \subset \mathbb{Z}[a, b]$, we see that $\mathbb{Z}[a + b]$ is finitely generated and being torsion free, it is free, say of some rank p. Multiplication by $a + b$ on $\mathbb{Z}[a + b]$ can be thought of as a $p \times p$ integer matrix. Let $P(X)$ be the characteristic (monic) polynomial of this matrix (of degree p) and then, $P(a + b) = 0$, showing $a + b$ is algebraic. Case of ab is identical. □

(4) Show that $\cos r\pi, \sin r\pi$ are algebraic, where $r \in \mathbb{Q}$ and the angles are in radians as usual. (De Moivre's theorem).

Solution. De Moivre says, $(\cos\theta + i \sin\theta)^n = \cos n\theta + i \sin n\theta$ for any $n > 0$. So, write $r = a/n$ with a, n integers and

$n > 0$. Since $\cos a\pi, \sin a\pi$ are integers, taking $\theta = r\pi$ above, we get $\cos r\pi + i \sin r\pi$ is algebraic. Similarly, taking $\theta = -r\pi$, one gets, $\cos r\pi - i \sin r\pi$ is algebraic. Adding, we get $2\cos r\pi, 2i \sin r\pi$ are both algebraic. The rest is clear, since $i \neq 0$ is also algebraic. □

(5) Let F be a finite field with say q elements.

(a) Show that the characteristic of F is a prime number p and $q = p^m$ for some m.

Solution. We know the characteristic must be a prime number, since the only other option is characteristic zero and then we have $\mathbb{Q} \subset F$ and in particular, F must be infinite. If it is p, we have $\mathbb{F}_p \subset F$ and F is a finite dimensional (F is finite!), say of dimennsion m, then clearly $q = p^m$. □

(b) Show that $a^q = a$ for all $a \in F$.

Solution. F^*, the non-zero elements of F form an abelian group of order $q - 1$ and thus for any $0 \neq a \in F$, we have $a^{q-1} = 1$ and thus $a^q = a$. If $a = 0$, this is trivial. □

(c) Let $F \subset L$ be a field extension and let $a \in L$ algebraic over F. Show that $a^{q^m} = a$ for some positive integer m.

Solution. We look at $F \subset F(a) \subset L$ and since a is algebraic, we see that $[F(a) : F]$ is finite, say m. Then F has q^m elements and so the result follows from the previous part. □