Algebra (Math 211) Final Questions and Solutions

Ali Nesin

January 11, 2004

1. *Let R be a ring with 1. Show that R has a maximal (and proper) ideal.* (5 pts.)

   Proof: Let Z be the set of proper ideals of R. Since the trivial ideal 0 is in Z, Z is nonempty. Order Z by inclusion. If $(I_i)_i$ is an increasing chain from Z, then $\cup_i I_i$ is also in Z since 1 cannot be in $\cup_i I_i$ (this is the important point: 1 exists! Otherwise the statement does ot hold as we will see. Also if $(I_i)_i$ were not a chain, it wouldn't be an ideal), not being in any of the I_i's. Thus Z is an inductive set and by Zorn's Lemma Z has a maximal element. Any maximal element of Z is a maximal ideal of R.

2. **a.** *Let G be an abelian group. Let $H < G$ be a proper maximal subgroup. Show that $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p.* (7 pts.) *Conclude that a divisible abelian group cannot have a maximal proper subgroup.* (7 pts.)

   Proof: Since H is a maximal subgroup, the quotient group G/H does not have a proper nontrivial subgroup. Now the first part of the question follows from the following:

   Claim: *Any group (abelian or not) that does not have a proper nontrivial subgroup is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

   Proof of the Claim: Let G be such a group. Then for any $g \in G$, $C_G(g) = G$, thus G is abelian. Since $G = \langle g \rangle$ for any $g \in G \setminus \{1\}$, G is cyclic. We cannot have $G \simeq \mathbb{Z}$, since otherwise G would have many subgroups corresponding to the subgroups $n\mathbb{Z}$, $n > 1$. Thus $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n > 0$. If p were a proper divisor of n, then $0 < p\mathbb{Z}/n\mathbb{Z} < \mathbb{Z}/n\mathbb{Z}$, a contradiction. Thus n is a prime. This proves the claim and the first part.

   Let now G be a divisible abelian group. Let $H < G$ be a maximal subgroup. Then, by the first part, $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ for some (prime) integer p. Let $g \in G$. Let $k \in G$ be such that $k^p = g$. Then in the quotient group G/H, $\overline{g} = \overline{k}^p = 1$, so that $g \in H$. Thus $G = H$.

   b. *Conclude from part a that there are rings (necessarily without 1) without maximal ideals.* (5 pts.)

Proof: Let G be any divisible group, e.g. $G = \mathbb{Q}^+$, $\mathbb{R}^+$ or $\mathbb{Z}_{p^\infty}$. Denote G additively. Define multiplication on I by decreeing $gh = 0$ all g, $h \in G$. Then G becomes a ring. An ideal of the ring G corresponds to a subgroup of the group G. Thus G – not having maximal subgroups – does not have maximal ideals.

c. *Let G be a group and $1 \neq a \in G$. Show that G has a subgroup which is maximal with respect to not containing a.* (4 pts.)

Proof: Exactly as in Question 1.

d. *Find a subgroup of $\mathbb{Q}^+$ which is maximal with respect to not containing 1.* (7 pts.)

Solution. Let p be any prime. Consider

$$H := \{a/b : a, b \in \mathbb{Z} \text{ such that } p \text{ divides } a \text{ but not } b\}.$$

Then H is a subgroup of $\mathbb{Q}^+$. Clearly $1 \notin H$ and $p \in H$. We claim that if $H < K \leq G$ then $1 \in K$. This will show that H is a maximal subgroup of $\mathbb{Q}$ not containing 1. Let $\gamma \in K \setminus H$. We can write $\gamma = c/d$ for some c, $d \in \mathbb{Z}$ with $(c, p) = 1$. There are x, $y \in \mathbb{Z}$ such that $cx + yp = 1$. Thus $1 = (dx)\gamma + yp \in \langle \gamma, H \rangle \leq K$.

3. *Let $R = X\mathbb{R}[X]$ considered as a ring (without 1). Let $I = X^2\mathbb{R}[X] \lhd X\mathbb{R}[X]$.*

a. *Show that R/I as an additive group is isomorphic to $\mathbb{R}^+$ and that the multiplication of R/I is the zero-multiplication (i.e. the product of any two elements of R/I is zero).* (3 pts.)

Proof: Consider the map $\phi : \mathbb{R} \longrightarrow R/I$ given by $\phi(a) = \overline{aX}$. This is certainly a homomorphism of additive groups.

ϕ is onto because for any $f(X) = f_0 + f_1X + ... + f_nX^n$, $\phi(f_0) = \overline{Xf(X)}$.

ϕ is one-to-one because if $a \in \ker(\phi)$, i.e. if $\phi(a) = \overline{0}$ then $\overline{aX} = \overline{0}$ and the second degree polynomial X^2 divides the first degree polynomial aX, which implies that $aX = 0$ and $a = 0$.

For the multiplication in R/I: Given any $\overline{Xf(X)}$, $\overline{Xg(X)} \in R/I$, we have $\overline{Xf(X)}\,\overline{Xg(X)} = \overline{X^2f(X)g(X)} = \overline{0}$.

b. *Conclude that R/I has no maximal ideals.* (4 pts.)

By part a, instead of R/I we may just consider the ring $\mathbb{R}$ with the usual addition and the zero multiplication. By the solution of part b of Question 2, $\mathbb{R}$ has no maximal ideals.

c. *Conclude that R has no maximal ideals.* (8 pts.)

Proof: Note first that I is not a maximal ideal of R (because otherwise $\overline{0}$ would be a maximal ideal of R/I, contradicting part b.

Let J be a maximal ideal of R. Since $(I+J)/I \lhd R/I$, either $I+J=I$ or $I+J=R$. In the first case $J \leq I$, making I a maximal ideal, a contradiction. Assume $I+J=R$.

I do not know how to continue... The question seems to be open for the moment. Does R have a maximal ideal? Is a maximal ideal of R that does not contain X a maximal ideal of R?

4. *Let $R=\mathbb{Z}[\sqrt{d}]$ where $d \neq 0, 1$ is a square-free element of $\mathbb{Z}$.*

a. *Show that the map $\_ : R \longrightarrow R$ defined by $\overline{a+b\sqrt{d}} = a-b\sqrt{d}$ for all $a, b \in \mathbb{Z}$ is a ring automorphism.* (2 pts.)

Proof: This is easy to show. We need to compute to check that $\overline{\alpha}+\overline{\beta} = \overline{\alpha+\beta}$, $\overline{\alpha}\,\overline{\beta} = \overline{\alpha\beta}$ for all $\alpha, \beta \in R$. The facts that the map $\_$ is onto and one-to-one is trivial.

b. *For $\alpha \in R$, let $N(\alpha) = \alpha\overline{\alpha}$. Show that $N(\alpha) \in \mathbb{Z}$ and that $N : R \longrightarrow \mathbb{Z}$ is multiplicative.* (2 pts.)

Proof: Since, for $a, b \in \mathbb{Z}$ and $\alpha = a+b\sqrt{d}$, $N(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2-db^2$, $N(\alpha) \in \mathbb{Z}$. Also, for any $\alpha\beta \in R$, $N(\alpha\beta) = (\alpha\beta)\overline{\alpha\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$.

c. *For $\alpha \in R$, show that $\alpha \in R^*$ if and only if $N(\alpha) = \pm 1$.* (5 pts.)

Proof: If $\alpha \in R^*$, then there is a $\beta \in R$ such that $\alpha\beta = 1$. Thus $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $N(\alpha), N(\beta) \in \mathbb{Z}$, this implies that $N(\alpha) = N(\beta) = \pm 1$.

Conversely, assume $N(\alpha) = \pm 1$. Then $(N(\alpha)\overline{\alpha})\alpha = N(\alpha)^2 = 1$ so that $N(\alpha)\overline{\alpha}$ is the inverse of α.

d. *For $\alpha \in R$, show that if $N(\alpha)$ is prime then α is irreducible.* (3 pts.)

Proof: Assume $N(\alpha)$ is prime. Let $\alpha = \beta\gamma$ where $\beta, \gamma \in R$. Then $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Since $N(\alpha)$ is prime, this implies that either $N(\beta)$ or $N(\gamma)$ is ± 1, i.e. either β or γ is invertible. Hence α is irreducible.

e. *Assume $d < -1$. Find R^*.* (3 pts.)

By part c, $R^* = \{\alpha \in R : N(\alpha) = \pm 1\}$. But $N(\alpha) = a^2 - db^2 = a^2 + |d|b^2$ for $\alpha = a+b\sqrt{d}$ and $a, b \in \mathbb{Z}$. So $N(\alpha) \geq |d| > 1$ if $b \neq 0$. Thus $R^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

f. *Assume $d = -1$. Find R^* and its group structure.* (5 pts.)

Proof: By part c, $R^* = \{a+b\sqrt{-1} : a, b \in \mathbb{Z}\ a^2+b^2 = 1\} = \{1, -1, i, -i\}$ where $i^2 = -1$. Since i has order 4, $R^* \simeq \mathbb{Z}/4\mathbb{Z}$.

e. *Show that the map $\_ : R \longrightarrow R$ defined above is the only nontrivial ring automorphism of R.* (5 pts.)

Proof: Any automorphism must be trivial on $\mathbb{Z}$, as usual. Thus it is enough to find the image of $\sqrt{d}$. Let $x = \sqrt{d}$. Then $x^2 = d$ and so $\phi(x)^2 = \phi(x^2) = \phi(d) = d$, hence $\phi(x) = \pm\sqrt{d}$.

5. *Let G be a finite abelian group. Show that if any p-subgroup of G is cyclic for any prime p then G is cyclic itself.* (5 pts.)

   Proof: G is the direct sum of its primary parts, which are all cyclic. We know that the product of finitely many cyclic groups of order two by two prime to each other is a cyclic group. (For this, it is enough to prove that if $(n, m) = 1$, then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/nm\mathbb{Z}$).

6. *Show that if $r \leq s$ then $X^{p^r} - 1$ divides $X^{p^s} - 1$.* (3 pts.)

   Proof: Let $s = r + t$ and $Y = X^{p^r}$. Then $X^{p^s} = X^{p^{r+t}} = X^{p^r p^s} = (X^{p^r})^{p^t} = Y^{p^t}$. Thus we need to show that $Y - 1$ divides $Y^{p^t} - 1$, but $Y - 1$ always divides $Y^n - 1$.

7. *Show that if F_1 and F_2 are two finite subfields of a field K of the same cardinality then $F_1 = F_2$.* (5 pts.)

   Proof: Say $|F_1| = |F_2| = n$. Then F_1^* and F_2^* are groups of order $n - 1$. Hence, for any $x \in F_1^* \cup F_2^*$, $x^{n-1} = 1$. It follows that for any $x \in F_1 \cup F_2$, $x^n = x$. Hence the elements of $F_1 \cup F_2$ are the roots of the polynomial $X^n - X$. But this polynomial has at most n roots. So $F_1 = F_2 = \{x \in K : x^n = x\}$. (In reality n is a prime power).

8. *Show that a finite subgroup of a field is cyclic.* (15 pts.)

   Proof: Let F be a field and G be a finite group of F^*. By decomposing G into its primary parts, we may assume that G is a p-group for some prime p. (Direct sum of finitely many cyclic groups whose orders are two by two relatively prime to each other is cyclic). Since any finite abelian p-group, for p prime, is a direct sum of cyclic p-subgroups, it is enough to show that G cannot be of the form $\mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}$ for some m, $n \geq 1$. Assume not. Then $\{x \in F : x^p = 1\}$ has at least $p^2 - 1$ elements, so the polynomial $X^p - 1$ has at least $p^2 - 1$ roots in the field F, more than p, a contradiction.

9. *Conclude from Question 8 that if $F \leq K$ are finite fields then $K = F[\alpha]$ for some $\alpha \in K$.* (3 pts.)

   Proof: Since K^* is a cyclic group, there is an $a \in K^*$ such that $K^* = \langle\alpha\rangle$. Then $K = F[\alpha]$ of course.